FINITE GROUPS WITH AUTOMORPHISMS INVERTING MANY ELEMENTS

A Thesis submitted for the degree of Doctor
of Philosophy at the University of Keele 1972.

by

PATRICK DESMOND MACHALE M.Sc. (N.U.I.)

DECLARATION

The material in this thesis is claimed as original except where explicitly stated otherwise. This thesis has not been submitted previously for a higher degree of this or any other University.

ACKNOWLEDGEMENTS

I wish to express my most sincere thanks to my supervisor, Dr. Hans Liebeck, for the wonderful way in which he has guided me and helped me during the past three years.

I wish to thank the University of Keele for its financial support and award of a Postgraduate Studentship.

I also wish to thank my parents for all the understanding, help, and opportunities they have given me.

Finally, I thank Mrs. Sheila Pye for her patience and excellent typing.

TO ANNE

CONTENTS

NOTATION AND TERMINOLOGY

G denotes a finite group and H and A are subgroups of G. A finite set T of group elements has $|T|$ distinct elements. If α is an automorphism of G we denote by S_α the elements of G which are inverted by α. We define

$$\ell(\alpha) = |S_\alpha|/|G| \text{ and } \ell(G) = \max_{\gamma \in \text{Aut } G} \ell(\gamma),$$

where Aut G denotes the full group of automorphisms of G. If $\ell(\alpha) = k$, we call α a k-automorphism and if $k > \frac{1}{2}$ we also say that α is a $> \frac{1}{2}$-automorphism. A group with a $> \frac{1}{2}$-automorphism is called a $> \frac{1}{2}$-group and a group with a k-automorphism is called a k-group, $0 < k \leq 1$. Given $x_i \in G$ $(i = 1, \ldots, r)$ and a subset T of G, $\langle x_1, \ldots, x_r, T \rangle$ denotes the subgroup generated by $x_1, \ldots, x_r$ and the elements of T. G_p is the set of all non-Abelian groups with order divisible by no prime less than the prime p.

$(G : H)$	is the index of the subgroup H in G.
$\alpha, \beta, \ldots,$	Automorphisms of a group G.
F_α	Subgroup of all elements fixed by α.
I_x	Inner automorphism $g \to x^{-1}gx$ for all $g \in G$.
$[a, b] = a^{-1}b^{-1}ab = a^{-1}a^b$.	$[a, b, c] = [[a, b], c]$
G'	is the commutator subgroup of G.
Z(G)	is the centre of G.
Q	The Quaternion group of order 8.
D_n	The dihedral group of order 2n.
S_n	The symmetric group on n symbols.
A_n	The alternating group on n symbols.
C_n	The cyclic group of order n.
A x B	The direct product of groups A and B.
A/B	The factor group of A modulo B.
$A \setminus B$	The set $\{a \mid a \in A, a \notin B\}$.
$N_G(A)$	The normalizer of the subgroup A in G.

/Cont'd...

Notation and Terminology cont'd..

A_α	A subgroup of maximum order in S_α.
$C_A(x)$	The centralizer in the subgroup A of the element x.
$m \mid n$	m divides n.
G^p	The subgroup generated by the pth powers of the elements of G.

ABSTRACT of the Thesis "Finite Groups with Automorphisms Inverting Many Elements"

by Patrick Desmond MacHale, University of Keele, 1972.

It is known that a group is Abelian if and only if it has an automorphism inverting every element. We consider finite non-Abelian groups with an automorphism inverting many elements.

Firstly, we consider the case where G is a group with an automorphism inverting more than $\frac{1}{2}|G|$ elements, a problem first considered by G. A. Miller in a series of papers. We prove that either G has an Abelian subgroup of index 2 (with no further restrictions) or G is nilpotent of class 2, with an elementary Abelian commutator subgroup of order 2 or 4. We also prove that if α_1 and α_2 are automorphisms of G which invert more than $\frac{1}{2}|G|$ elements, then both α_1 and α_2 invert $\frac{q+1}{2q}|G|$ elements for some positive integer q.

As a special case we obtain the structure of groups in which the identity automorphism inverts more than half the elements. These are precisely the groups in which at least half the elements are involutions. This problem was also considered by G. A. Miller and more recently by C. T. C. Wall who used character theory to obtain a classification.

Next we consider groups G of odd order, where no prime less than the prime p divides $|G|$. When G is non-Abelian we show that no automorphism can invert more than $\frac{1}{p}|G|$ elements of G and we obtain a complete classification of all groups G with an automorphism inverting exactly $\frac{1}{p}|G|$ elements. We prove that either G has an Abelian subgroup of index p which does not contain all the elements of order p or G is nilpotent of class 2 with commutator subgroup of order p and $G' \cap G^p = 1$ or $G/Z(G)$ is non-Abelian of order p^3 and exponent p.

Next we obtain a complete classification of groups G with an automorphism inverting exactly $\frac{1}{2}|G|$ elements. If G is non-Abelian, we show that G has an Abelian subgroup of index 2 or 4 or G has commutator subgroup of order 2. The classification divides into many cases as detailed in the structure theorems.

All the groups considered are close to being Abelian in some sense i.e. they are soluble and have either Abelian subgroups of small index, large centres, or small commutator subgroups. Let $\ell(G)$ be the greatest proportion of elements of a finite group G that are inverted by an automorphism. Thus $\ell(G) = 1$ if and only if G is Abelian and we have classified groups for which $\ell(G) > \frac{1}{2}$, $\ell(G) = \frac{1}{2}$, and $\ell(G) = \frac{1}{p}$, where p is the least prime which divides $|G|$.

/Cont'd...

Let $k(G)$ be the number of conjugacy classes in G and let $R(G) = k(G)/|G|$. K. S. Joseph has studied the properties of the function $R(G)$ and used its value as a measure of the commutativity of G, since it is the probability that a pair of elements chosen at random from G commute with each other. We use $\ell(G)$ as another measure of commutativity and show that when $\ell(G) \geq \frac{1}{2}$ or when $G \in G_p$ (p odd) and $\ell(G) = \frac{1}{p}$ then $R(G)$ is large also.

Finally, we define a C-set of a finite group to be a subset S of G such that given $s_1, s_2 \in S$, then $s_1 s_2 \in S$ if and only if s_1 and s_2 commute. If S is a C-set of maximum order in G we define $b(G)$ to be $|S|/|G|$ and we use $b(G)$ as another measure of commutativity. We show that if p is the least prime which divides $|G|$ then $b(G) \leq \frac{2p-1}{p^2}$ if G is non-Abelian, with equality if and only if $G/Z(G)$ has order p^2. We examine groups with $b(G) > \frac{1}{2}$ and show that G is soluble. We also show that if a C-set contains more than $\frac{1}{2}|G|$ elements of G, then it contains $\frac{q+1}{2q}|G|$ elements for some positive integer q and we derive some results on the structure of G.

INTRODUCTION

It is well known that a group is Abelian if and only if it has an automorphism inverting all its elements. We are concerned with finite non-Abelian groups in which some automorphism inverts a large proportion of the elements of the group. For groups of even order, we find the complete structure of groups G with an automorphism inverting at least $\frac{1}{2}|G|$ elements. If G has odd order we show that no automorphism can invert more than $\frac{1}{p}|G|$ elements, where p is the least prime which divides $|G|$. Finally, we give a complete classification of all groups G with an automorphism inverting exactly $\frac{1}{p}|G|$ elements, where p is the least prime which divides $|G|$.

All the groups we consider are in some sense "close to being Abelian" and we are led to define and compare certain measures of commutativity in finite groups.

Many of the ideas in this thesis are based on the work of G. A. Miller who first attempted to solve some of the problems we look at. His analysis was incomplete and difficult to follow and indeed some of his results are somewhat in conflict with ours.

The material of CHAPTER 1 of this thesis has already appeared in published form [16] and the material of CHAPTER 2 has been accepted for publication [17].

CHAPTER 1. GROUPS WITH $>\frac{1}{2}$-AUTOMORPHISMS

SECTION (1.1) Introductory Remarks

We begin by giving a complete classification of non-Abelian groups G with an automorphism inverting more than $\frac{1}{2}|G|$ elements. We prove that either they possess an Abelian subgroup of index 2 (with no further restriction) or they are nilpotent of class 2 of a special type, as detailed in Theorem 1.3.13 .

Our problem has attracted the attention of a number of authors in the early part of this century. In 1906 Manning [7] proved that a group G has an automorphism inverting exactly $\frac{3}{4}|G|$ elements if and only if $(G : Z(G)) = 4$. He also showed that if a group has a k-automorphism with $k \geq \frac{5}{8}$ then $k = \frac{5}{8}, \frac{2}{3}, \frac{3}{4}$, or 1. Miller [8] obtained similar results and considered more generally the properties of groups with a k-automorphism, $k > \frac{1}{2}$.

We extend Manning's result by showing that if G has a k_1-automorphism and a k_2-automorphism, $k_1 > \frac{1}{2}$, $k_2 > \frac{1}{2}$, then $k_1 = k_2 = \frac{q+1}{2q}$ for some positive integer q.

Section (1.2) Preliminary Theorems

(1.2.1) Lemma. Given $\alpha \in$ Aut G and $s \in S_\alpha$, let I_s be the inner automorphism defined by $gI_s = s^{-1}gs$, $g \in G$. Then S_β, the set of elements of G inverted by the automorphism $\beta = I_s\alpha$, is given by

$$S_\beta = S_\alpha s^{-1} = s S_\alpha \text{ and thus } \ell(\beta) = \ell(\alpha).$$

Proof. $g(I_s\alpha) = g^{-1}$ iff $(s^{-1}gs)\alpha = g^{-1}$ iff $(gs)\alpha = (gs)^{-1}$ iff $gs \in S_\alpha$. Therefore $S_\beta = S_\alpha s^{-1}$. The second equality follows similarly.

(1.2.2) Subgroup Theorem. Let H be a subgroup of a $> \frac{1}{2}$-group G. Then there is a $> \frac{1}{2}$- automorphism of G that inverts more than half the elements of H (and so maps H onto itself). Moreover $\ell(H) \geq \ell(G)$.

Proof. Let α be a $> \frac{1}{2}$-automorphism of G. Since $|S_\alpha| = \ell(\alpha)|G|$, it

follows that some coset of H in G, Hs say, has at least $\ell(\alpha)|Hs|$ elements in S_α. We may clearly choose the coset representative s in S_α. From the inequality

$$|Hs \cap S_\alpha| \geq \ell(\alpha)|Hs|$$

it follows that

$$|H \cap S_\alpha s^{-1}| \geq \ell(\alpha)|H|.$$

Put $\beta = I_s\alpha$. Then, by Lemma (1.2.1) $\ell(\beta) = \ell(\alpha)$ and

$$|H \cap S_\beta| \geq \ell(\beta)|H|.$$

Thus β inverts more than half the elements of H. Denote by $\beta|H$ the automorphism of H induced by β. Then

$$\ell(\beta|H) = \frac{|H \cap S_\beta|}{|H|} \geq \ell(\beta).$$

It follows that if we choose α such that $\ell(\alpha) = \ell(G)$, then $\ell(\beta|H) \geq \ell(\beta) = \ell(G)$ and so $\ell(H) \geq \ell(G)$.

The following corollary is an immediate consequence of the subgroup theorem.

(1.2.3) Corollary. If H is an Abelian subgroup of a $> \frac{1}{2}$-group G then there is a $> \frac{1}{2}$-automorphism of G which inverts H elementwise.

Abelian subgroups play a fundamental role in the structure of $> \frac{1}{2}$-groups and we proceed to study them in some detail.

(1.2.4) Lemma. Let β be a $> \frac{1}{2}$-automorphism of G that inverts an Abelian subgroup H elementwise. Suppose that the coset Hg has non-trivial intersection with S_β. Then the number of elements in Hg that are inverted by β is $|C_H(g)|$, the order of the centralizer of g in H.

Proof. By hypothesis $Hg \cap S_\beta$ is not empty, so we may choose $s \in S_\beta$ such that $Hg = Hs$. Now for $h \in H$, $(hs)\beta = (hs)^{-1}$ if and only if $h^{-1}s^{-1} = s^{-1}h^{-1}$. Hence

$$Hg \cap S_\beta = (C_H(s))s.$$

But $C_H(s) = C_H(g)$, and the lemma follows.

(1.2.5) Transversal Theorem. Let β be a $> \frac{1}{2}$-automorphism of G that inverts the Abelian subgroup H elementwise. If H is a maximal subgroup of S_β (i.e. H is not contained properly in a subgroup of G lying entirely in S_β) then there exists a decomposition of G relative to cosets of H

$$G = Hs_1 \cup Hs_2 \cup \ldots \cup Hs_n, \quad s_1 = 1,$$

such that $s_i \in S_\beta$ $(i = 1, \ldots, n)$.

Proof. Suppose that Hg contains an element $s \in S_\beta$; then $Hg = Hs$, and s may be chosen as coset representative. Now if $Hs \neq H$ then $C_H(s)$ must be a proper subgroup of H, for otherwise $\langle s, H \rangle$ lies in S_β and properly contains H, contrary to hypothesis. By Lemma (1.2.4), at most half the elements of Hg belong to S_β. Hence if some coset of H in G contained no elements of S_β then $|S_\beta|$ could not exceed $\frac{1}{2}|G|$. Since β is a $> \frac{1}{2}$-automorphism, every coset must contain an element of S_β and the theorem is proved.

(1.2.6) Centralizer Theorem. Let H be a maximal subgroup of S_β where β is a $> \frac{1}{2}$-automorphism of G. Let

$$G = H \cup Hg_2 \cup \ldots \cup Hg_n \tag{1.2.7}$$

be a composition of G relative to cosets of H. Put

$$q_i = (H : C_H(g_i))$$

Then

$$|S_\beta| = |H| + \sum_{i=2}^{n} |C_H(g_i)|, \text{ where } q_i \geq 2 \ (i = 2, \ldots, n). \tag{1.2.8}$$

Moreover, the following inequality on the indices q_i holds.

$$\sum_{i=2}^{n} \left(\frac{1}{2} - \frac{1}{q_i}\right) < \frac{1}{2}. \tag{1.2.9}$$

Proof. Formula (1.2.8) follows from Lemma (1.2.4) and Theorem (1.2.5). The inequality (1.2.9) is a consequence of the fact that $|S_\beta| > \frac{1}{2}n|H|$.

(1.2.10) Corollary. An automorphism which inverts more than half the elements of a group G inverts exactly $\ell(G)|G|$ elements.

Proof. Let α be a $> \frac{1}{2}$-automorphism of G, and let H be an arbitrary maximal Abelian subgroup of G. By the Subgroup Theorem (1.2.2) and Corollary (1.2.3), there exists an automorphism β that inverts H elementwise and such that $\ell(\beta) = \ell(\alpha)$. Since H is maximal Abelian in G it is certainly a maximal subgroup of S_β. Therefore by (1.2.8)

$$|S_\alpha| = |S_\beta| = |H| + \sum_{i=2}^{n} |C_H(g_i)|, \tag{1.2.11}$$

where we suppose that G admits a coset decomposition (1.2.7). But the number given by the right hand side of (1.2.11) is independent of α; so any $> \frac{1}{2}$-automorphism must invert this number of elements.

Hence we obtain a formula which relates this number to the Abelian subgroup structure of G: If H is an arbitrary maximal Abelian subgroup of a $> \frac{1}{2}$-group G, then

$$\ell(G)|G| = |H| + \sum_{i=2}^{n} |C_H(g_i)|,$$

where G admits a coset decomposition (1.2.7).

As a consequence of the centralizer inequality (1.2.9) we can easily impose conditions on the maximal Abelian subgroups of a $> \frac{1}{2}$-group G and restrictions on the values of numbers q_i. Suppose a maximal Abelian subgroup H has index n in G. Then relative to a suitable ordering of the cosets of H in G only the following cases can possibly arise:

$$\begin{array}{ll} \text{I} & n = 2; \\ \text{II} & n \geq 3,\ q_i = 2\ (i = 2, \ldots, n); \\ \text{III} & n \geq 3,\ q_2 \geq 3,\ q_i = 2\ (i = 3, \ldots, n); \\ \text{IV} & n \geq 3,\ q_2 = 3,\ q_3 = 4 \text{ or } 5,\ q_i = 2\ (i = 4, \ldots, n); \\ \text{V} & n \geq 3,\ q_2 = q_3 = 3,\ q_i = 2\ (i = 4, \ldots, n). \end{array} \tag{1.2.12}$$

In order to show that some of these possibilities do not arise in $> \frac{1}{2}$-groups we need some further results concerning the Abelian subgroup structure of $> \frac{1}{2}$-groups.

(1.2.13) The Squares Theorem. Let H be a subgroup of maximum order in S_β, where β is a $> \frac{1}{2}$-automorphism of G. Then the square of every element in S_β belongs to H.

Proof. Suppose $s \in S_\beta$ but $s \notin H$. We must show $s^2 \in H$. If $(G : H) = 2$ the result is clear. So we may suppose that $(G : H) = n \geq 3$. We first consider the case $(H : C_H(s)) = 2$. The group $H_1 = \langle s, C_H(s) \rangle$ is contained in S_β. If s^2 does not belong to $C_H(s)$ then $|H_1| \geq 3|C_H(s)|$; but $|H| = 2|C_H(s)|$ and so H does not have maximum order in S_β, contrary to hypothesis. We conclude that $s^2 \in C_H(s) \subset H$.

We next consider the case $q = (H : C_H(s)) \geq 3$. If s^2 does not belong to H then Hs and Hs^{-1} are distinct cosets. Since $C_H(s) = C_H(s^{-1})$ the only possible structure of G is subject to condition (1.2.12)V. In particular

$$(1.2.14) \qquad (H : C_H(s)) = (H : C_H(s^{-1})) = 3.$$

We may suppose that s^3 belongs to $C_H(s)$, for otherwise $\langle s, C_H(s) \rangle$, which belongs to S_β, has order greater than that of H.

We may put $G_1 = \langle s, H \rangle$. Two possibilities arise:

Case (i) H is normal in G_1; here β inverts $s^{-1}hs$ for all h in H, that is

$$s^{-1}h^{-1}s = (s^{-1}hs)^{-1} = (s^{-1}hs)\beta = sh^{-1}s^{-1}.$$

Hence s^2 commutes with every element of H and thus s^2 is contained in H, which is contrary to hypothesis.

Case (ii) H is not normal in G_1; in this case $s^{-1}Hs \neq H$. We choose an element $h \in H$ such that $h \notin C_H(s)$. Then by (1.2.14),

$$H = \langle h, C_H(s) \rangle, \quad h^3 \in C_H(s).$$

Now

$$C_H(s) = C_H(sh) = C_H(sh^2)$$

and so each of these centralizers has index 3 in H. Since G must satisfy condition (1.2.12)V, two of the three cosets Hs, Hsh, Hsh^2 must be equal. But it is easy to see that this implies that H is normal in G_1, contrary to hypothesis.

We conclude that s^2 must belong to H, and the proof is complete.

(1.2.15) The Index 2 Theorem, Let A be an Abelian subgroup of maximum order in G. Let β be a $> \frac{1}{2}$-automorphism that inverts A elementwise.

Then for $s \in S_\beta$, $s \notin A$, A has index 2 in $\langle s, A \rangle$.

Proof. Put $G_1 = \langle s, A \rangle$ and $(G_1 : A) = n$. Two cases arise.

Case (i) $(A : C_A(s)) = 2$. The centre of G_1 is $Z = C_A(s)$, and G_1/Z has order 2n with a subgroup A/Z of order 2. Now if G_1/Z contains a coset bZ of order $m > 2$, then $B = \langle b, Z \rangle$ is Abelian and $|B| = m|Z| > 2|Z| = |A|$, which contradicts the definition of A. Therefore G_1/Z is elementary Abelian, and so A is a normal subgroup of G_1. By the SquaresTheorem (1.2.13), $s^2 \in A$ and hence $n = 2$.

Case (ii) $q = (A : C_A(s)) \geq 3$. Suppose by way of contradiction that $n > 2$. Then besides A and As there exists a third coset of A in G_1, and, since $As^2 = A$, it must be of the form Asa for some $a \in A$, $a \notin C_A(s)$. Now $C_A(s) = C_A(sa)$ and so G_1 must satisfy condition (1.2.12)V. Therefore $q = 3$ and

$$A = \langle a, C_A(s) \rangle, \quad a^3 \in C_A(s).$$

But we also have $C_A(s) = C_A(sa^2)$ and so, according to (1.2.12)V, two of the three cosets As, Asa, Asa^2 are equal. From this we find easily that A is normal in G_1. But $s^2 \in A$ and so $n = 2$. This contradiction completes the proof.

(1.2.16) Remark. In the last theorem we required A to be an Abelian subgroup of maximum order in G. The assumption that A be of maximum order in S_β (as was required in the Squares Theorem) is not sufficient. For example, in the symmetric group on three symbols, the identity automorphism, ι, is a $\frac{2}{3}$-automorphism, and $H = \langle (12) \rangle$ is a subgroup of maximum order in S_ι. The permutation $s = (13)$ belongs to S_ι, but H has index 3 in $\langle s, H \rangle$.

We reserve the letter A to denote an Abelian subgroup of maximum order in G.

SECTION (1.3) The structure of Non-Abelian $> \frac{1}{2}$-groups

The results of section(1.2) relate the subgroup structure of a $> \frac{1}{2}$-group G to sets of elements inverted by a $> \frac{1}{2}$-automorphism. We are now able to

develop properties of G that do not refer to specific automorphisms. Finally we obtain a complete classification of all non-Abelian $> \frac{1}{2}$-groups.

Throughout this section G denotes a $> \frac{1}{2}$-group and A is an Abelian subgroup of maximum order in G.

(1.3.1) Theorem. The subgroup A is normal in G and G/A is an elementary Abelian 2-group.

Proof. By Corollary (1.2.3) there is a $> \frac{1}{2}$-automorphism β that inverts A elementwise. By the Transversal Theorem (1.2.5) every element $g \in G$ is expressible in the form $g = as$ for some $a \in A$, $s \in S_\beta$. Clearly $g^{-1}Ag = s^{-1}As$. Now suppose $g \notin A$. Put $G_1 = \langle s, A \rangle$. By theorem (1.2.15), $(G_1 : A) = 2$. Thus A is normal in G_1 and so $g^{-1}Ag = s^{-1}As = A$. Since g is arbitrary, it follows that A is normal in G. Moreover

$$g^2 = (as)^2 = (as^2)(s^{-1}as)$$

and so, by the Squares Theorem (1.2.13), $g^2 \in A$. Thus G/A is an elementary Abelian 2-group.

(1.3.2) Centralizer Structure Theorem. Let $G = A \cup Ag_2 \cup \ldots \cup Ag_n$ be a decomposition of G into a union of disjoint cosets of A, and put $q_i = (A : C_A(g_i))$ $(i = 2, \ldots, n)$. Then, relative to a suitable ordering of the cosets, one of the following conditions must hold (the corresponding values of $\ell(G)$ are indicated in brackets).

I^* $\quad n = 2$; $\left(\ell(G) = \frac{q_2 + 1}{2q_2}\right)$

II^* $\quad n = 2^k$ $(k \geq 2)$, $q_i = 2$ $(i = 2, \ldots, 2^k)$; $\left(\ell(G) = \frac{2^k + 1}{2^{k+1}}\right)$

III^* $\quad n = 4$, $q_2 = 4$, $q_3 = q_4 = 2$; $\left(\ell(G) = \frac{9}{16}\right)$.

Proof. We have already established conditions (1.2.12) and it remains to show that some of the cases listed there are not possible in $> \frac{1}{2}$-groups. Firstly by Theorem (1.3.1), the index n must be a power of 2. Next we rule out conditions (1.2.12) IV and V. For suppose that $q_2 = (A : C_A(g_2)) = 3$ and $q_3 = (A : C_A(g_3)) = 3$, 4 or 5. Since G/A is elementary Abelian, the

cosets Ag_2, Ag_3, and Ag_2g_3 are distinct. Assuming that condition IV or V holds, we must have $(A : C_A(g_2g_3)) = 2$. Now, since $g_2^2 \in A$,

$$C_A(g_3) = C_A(g_2^2 g_3) \supseteq C_A(g_2) \cap C_A(g_2g_3) = B, \text{ say.}$$

Clearly B has index 6 in A and so $C_A(g_3)$ cannot have index 4 or 5 in A. So we may assume $q_2 = q_3 = 3$. But then

$$C_A(g_2g_3) \supseteq C_A(g_2) \cap C_A(g_3) = C, \text{ say,}$$

where C has index 3 or 9 in A. Since C cannot be contained in a subgroup of index 2 in A, the case $q_2 = q_3 = 3$ is ruled out.

Next we consider condition III. Firstly, from the condition $q_i = 2$ $(i \geq 3)$ it follows that $q_2 = 2$ or 4, for

$$C_A(g_2) = C_A(g_2 g_3^2) \supseteq C_A(g_2g_3) \cap C_A(g_3),$$

and since g_2g_3 may be taken as the fourth coset representative, this last intersection has index 2 or 4 in A.

The case $n = 4$, $q_2 = 4$, $q_3 = q_4 = 2$ arises in $>\frac{1}{2}$-groups, but $n = 2^k$ $(k > 2)$, $q_2 = 4$, $q_i = 2$ $(i = 3, \ldots, 2^k)$ is impossible as we now prove.

It is convenient at this point to introduce a notation that exhibits G/A as an elementary Abelian 2-group. Suppose G/A has order 2^k $(k > 2)$ and is generated by x_1A, x_2A, ..., x_kA. We select x_1 such that $(A : C_A(x_1)) = 4$ and assume that $(A : C_A(x)) = 2$ for all $x \notin A \cup x_1A$. Our proof is based on the following observation.

(1.3.3) Suppose $xA \neq yA$ and $C_A(x)$, $C_A(y)$ both have index 2 in A. Then

$$C_A(x) = C_A(y) \Rightarrow C_A(xy) = C_A(x).$$

For, under the hypothesis, $C_A(xy) \supseteq C_A(x) \cap C_A(y) = C_A(x)$, and since $xy \notin A$, the possibility $C_A(xy) = A$ is ruled out.

Now the elements x_2, x_3, x_2x_3, x_1x_2, x_1x_3, and $x_1x_2x_3$ belong to distinct cosets and their centralizers in A have index 2 in A. Moreover

$$C_A(x_1) = C_A(x_1x_2^2) \supseteq C_A(x_1x_2) \cap C_A(x_2)$$

and since $C_A(x_1)$ has index 4 in A, we have equality here. By an

extension of this argument we obtain

$$C_A(x_1) = C_A(x_1x_2) \cap C_A(x_2) = C_A(x_1x_3) \cap C_A(x_3) = C_A(x_1x_2x_3) \cap C_A(x_2x_3).$$

Thus the centralizer in A of each of the 6 listed elements contains $C_A(x_1)$ and

$$(1.3.4) \quad C_A(x_1x_2) \neq C_A(x_2),\ C_A(x_1x_3) \neq C_A(x_3),\ C_A(x_1x_2x_3) \neq C_A(x_2x_3).$$

Now $A/C_A(x_1)$ is elementary Abelian of order 4 and so contains 3 subgroups of index 2.

Therefore the centralizers of the 6 listed elements are distributed among a set of three subgroups of index 2 in A. By (1.3.3), either $C_A(x_2)$, $C_A(x_3)$, and $C_A(x_2x_3)$ are all equal or they are all different. Both cases easily lead to a contradiction of (1.3.4) by application of (1.3.3). This shows that $(G : A) = n > 2^k$ $(k > 2)$ is not possible and completes the proof of the theorem.

With the help of Theorem (1.3.2) we will be able to obtain a complete classification of $> \frac{1}{2}$-groups. We shall see that each of the cases I^*, II^* and III^* leads to a class of such groups, which we call groups of types 1, 2 and 3 respectively.

Firstly, every group G of type 1 has a $> \frac{1}{2}$-automorphism. G contains an Abelian subgroup A of index 2 in G. Let $G = A \cup Ax$. The mapping

$$a \to a^{-1},\ ax \to a^{-1}x^{-1},\ a \in A$$

defines a $\frac{q+1}{2q}$-automorphism whose inverted set is $A \cup (C_A(x))x$, where $q = (A : C_A(x))$.

To determine the $> \frac{1}{2}$-groups of type 2 and 3 we require further analysis.

(1.3.5) Theorem. Let G be a $> \frac{1}{2}$-group of type 2 or 3. If x and y lie in different cosets of A in G, then $C_A(x) \neq C_A(y)$.

Proof. Assume to the contrary that $Ax \neq Ay$, but $C_A(x) = C_A(y)$. Then neither x nor y belongs to A and $(A : C_A(x)) = 2$. Let $G_1 = \langle x, y, A \rangle$. By Theorem (1.2.2), G_1 is a $> \frac{1}{2}$-group and it is clearly of type 2 or 3. Now

$$C_A(xy) \supseteq C_A(x) \cap C_A(y) = C_A(x).$$

But $xy \notin A$, and so $C_A(xy) = C_A(x)$.

Thus we have

$$C_A(x) = C_A(y) = C_A(xy) = Z, \text{ say,}$$

where $(A : Z) = 2$. This is a contradiction if G_1 is of type 3 and since in that case $G_1 = G$, we may assume for the rest of the proof that G and G_1 are both type 2.

Clearly Z is the centre of G_1 and since it has index 2 in A we may put $A = \langle a_1, Z \rangle$ with $a_1^2 \in Z$. We observe that $C_{G_1}(a_1) = A$, for A must be self-centralizing. In particular

(1.3.6) $$x^{-1}a_1x = a_1z_1, \; y^{-1}a_1y = a_1z_2,$$

where z_1 and z_2 are distinct elements of order 2 in Z.

Now $z_1 \neq z_2$, since yx^{-1} does not commute with a_1.

We note further that

(1.3.7) $$xy \neq yx$$

for if x and y commute then $\langle x, y, Z \rangle$ is Abelian and has order $2|A|$ which contradicts the choice of A.

Let α be a $> \frac{1}{2}$-automorphism of G_1 that inverts A elementwise. By the Transversal Theorem (1.2.5) we may suppose that α inverts both x and y, and so

(1.3.8) $$(axy)\alpha = a^{-1}x^{-1}y^{-1} \text{ for all } a \in A.$$

Now α inverts half of the elements of the coset Axy and since by (1.3.7) and (1.3.8) no element of Zxy is inverted, we must have

$$(a_1xy)^{-1} = (a_1xy)\alpha = a_1^{-1}x^{-1}y^{-1}.$$

It follows from (1.3.6) that

$$a_1xy = yxa_1 = a_1z_1z_2yx,$$

and thus $[x, y] = z_1z_2$.

Now $[xa_1, ya_1] = [x, y][x, a_1][a_1, y] = z_1z_2z_1z_2 = 1$.

Therefore $\langle xa_1, ya_1, Z \rangle$ is Abelian and has order $2|A|$. We have obtained a contradiction, and the proof is complete.

(1.3.9) Corollary. Suppose that G is a $\geqslant \frac{1}{2}$-group of type 2 or 3 such that G/A is elementary Abelian of order 2^k ($k \geqslant 2$) and

$$G/A = \langle x_1A, x_2A, \ldots, x_kA \rangle .$$

Put $Z = C_A(x_1) \cap C_A(x_2) \cap \ldots \cap C_A(x_k)$. Then Z is the centre of G and $(A : Z) = 2^k$. Moreover A/Z is elementary Abelian.

Proof. It is clear that Z is the centre of G and that $|A/Z| \leqslant 2^k$. Consider first G of type 2. By Theorem (1.3.5) A/Z has $2^k - 1$ distinct subgroups of index 2. Therefore by a known theorem it must be elementary Abelian of order 2^k. (Zassenhaus [15]).

Finally if G has type 3 then two of the centralizers $C_A(x_1)$, $C_A(x_2)$, $C_A(x_1x_2)$ have index 2 in A and intersect in the third, which is equal to Z. Thus in this case A/Z has order 4 and is elementary Abelian.

Our next result concerns the action of G/A on A.

(1.3.10) Lemma. Let G and G/A be defined as in Corollary (1.3.9), and suppose that if G is of type 3, generators x_1 and x_2 are so chosen that $C_A(x_1)$ and $C_A(x_2)$ have index 2 in A. Then for $i = 1, \ldots, k$ there exist $a_i \in A$ and $z_i \in Z$ such that

$$[a_i, x_i] = z_i, \quad [a_i, x_j] = 1, \quad (j \neq i)$$

with $z_i \neq 1$, $z_i^2 = 1$.

Moreover, if G has type 2 then $z_1 = z_2 = \ldots = z_k$, whereas if G has type 3 then $z_1 \neq z_2$.

Proof. Put $D_i = C_A(x_1) \cap \ldots \cap C_A(x_{i-1}) \cap C_A(x_{i+1}) \cap \ldots \cap C_A(x_k)$

Now $(D_i : Z) = 2$ and $C_A(x_i) \cap D_i = Z$, so we may choose $a_i \in D_i \setminus C_A(x_i)$, with the property that $[a_i, x_j] = 1$ when $j \neq i$ and $[a_i, x_i] \neq 1$. We now show that $[a_i, x_i] \in Z$.

From a well known commutator identity we obtain

$[x_i^{-1}, x_j^{-1}, a_i]^{x_j} [x_j, a_i^{-1}, x_i^{-1}]^{a_i} [a_i, x_i, x_j]^{x_i^{-1}} = 1$, and since $[x_i^{-1}, x_j^{-1}] \in A$ and $[x_j, a_i^{-1}] = 1$ ($i \neq j$), it follows that $[a_i, x_i] \in D_i$.

Moreover since $[a_i, x_i^2] = 1 = [a_i^2, x_i]$ we conclude that $[a_i, x_i] \in C_A(x_i)$.

Hence $[a_i, x_i] \in C_A(x_i) \cap D_i = Z$, which leads to the first statement of the lemma.

Suppose now that G has type 2. Consider the centralizer $C_A(x_i x_j)$ for $i \neq j$. By what has already been proved this group contains a_m ($m \neq i$ or j) but does not contain a_i or a_j. Since it has index 2 in A, we are forced to the conclusion that $a_i a_j \in C_A(x_i x_j)$. Thus

$$1 = [x_i x_j, a_i a_j] = z_i z_j,$$

and so $z_i = z_j$.

On the other hand, if G has type 3 then $C_A(x_1 x_2)$ has index 4 in A and $[x_1 x_2, a_1 a_2] \neq 1$, giving $z_1 \neq z_2$. This completes the proof.

An immediate consequence of Lemma (1.3.10) is

(1.3.11) Corollary. For $> \frac{1}{2}$-groups G not of type 1, $[G, A]$ lies in the centre of G and has order 2 or is non-cyclic of order 4 according as G has type 2 or 3.

We need one further result before we can give the structure of $> \frac{1}{2}$-groups.

(1.3.12) Lemma. With the notation of Corollary (1.3.9) and Lemma (1.3.10), the elements $x_1, x_2, \ldots, x_k$ can be chosen to commute pairwise.

Proof. Consider first G of type 2. By Corollary (1.3.11), $[G, A]$ is generated by an element z, say, which belongs to Z and has order 2. We show first that for all i, j, $[x_i, x_j] = z$ or 1. For consider $A_j = \langle x_j, C_A(x_j) \rangle$. This is an Abelian subgroup of maximum order in G, for clearly $|A_j| = |A|$. By Theorem (1.3.1), A_j is normal in G and G/A_j is elementary Abelian, generated by $a_j A_j$, and the cosets $x_i A_j$ for all $i = 1, \ldots, k$ except $i = j$. By Corollary (1.3.11), $[G, A_j]$ has order 2, and since it contains $[a_j, x_j] = z$, we conclude that $[G, A_j] = \langle z \rangle$. Therefore $[x_i, x_j] = z$ or 1.

We can now prove by induction that the coset representatives $x_1, \ldots, x_k$ of $Ax_1, \ldots, Ax_k$ can be so chosen that for $i = 1, \ldots, k$, x_i commutes

with x_j ($j = 1, \ldots, k$). Consider the case $i = 1$. If $[x_1, x_j] = z$, then we replace x_j by $a_1 x_j$ as coset representative of Ax_j, and obtain $[x_1, a_1 x_j] = [x_1, a_1][x_1, x_j] = z^2 = 1$. We note that the elements $a_1, \ldots, a_k$ constructed in Lemma (1.3.10) satisfy the same commutator relations with the new coset representatives as they did with the old.

Now suppose that we have already chosen $x_1, \ldots, x_k$ such that $x_1, x_2, \ldots, x_{i-1}$ commute with x_j ($j = 1, \ldots, k$). In particular then x_i commutes with each of $x_1, \ldots, x_{i-1}$. For every $j > i$ such that $[x_i, x_j] = z$ we replace x_j by $a_i x_j$ and obtain $[x_i, a_i x_j] = z^2 = 1$. Thus we construct new coset representatives which commute with x_i, and since they clearly commute with each of $x_1, \ldots, x_{i-1}$, the proof by induction is complete.

If G has type 3, we form $A_1 = \langle x_1, C_A(x_1) \rangle$ and by an argument similar to the above we conclude that $[x_1, x_2] = 1, z_1, z_2$ or $z_1 z_2$. Depending on which case occurs we find that one of the following pairs of coset representatives commute: $\{x_1, x_2\}$, $\{x_1, a_1 x_2\}$, $\{a_2 x_1, x_2\}$, $\{a_2 x_1, a_1 x_2\}$. This completes the proof.

We summarise our findings in the following theorem.

(1.3.13) Structure Theorem. A non-Abelian $> \frac{1}{2}$-group G is one of the following types.

Type 1. G has an Abelian subgroup A of index 2 in G. For every such group if $G = A \cup Ax$ then the map: $(a)\alpha = a^{-1}$, $(ax)\alpha = a^{-1}x^{-1}$ for all $a \in A$ defines a $> \frac{1}{2}$-automorphism of G with

$$\ell(\alpha) = \ell(G) = \frac{q+1}{2q}, \text{ where } q = (A : C_A(x)).$$

Type 2. G is nilpotent of class 2. It has commutator subgroup $\langle z \rangle$ of order 2. Its centre Z has index 2^{2k} ($k \geq 2$) in G, and G/Z is an elementary Abelian 2-group, generated by $x_1 Z, x_2 Z, \ldots, x_k Z, a_1 Z, a_2 Z, \ldots, a_k Z$, subject to the following commutator relations:

$$[x_i, x_j] = [a_i, a_j] = 1 \text{ for all } i, j = 1, \ldots, k.$$

$$[a_i, x_j] = 1 (i \neq j), \quad [a_i, x_i] = z.$$

Every such group has a $> \frac{1}{2}$-automorphism α defined by the map:

$$(ax_1^{\varepsilon_1}x_2^{\varepsilon_2}\ldots x_k^{\varepsilon_k})\alpha = a^{-1}x_1^{-\varepsilon_1}x_2^{-\varepsilon_2}\ldots x_k^{-\varepsilon_k}$$

for all $a \in A = \langle a_1, \ldots, a_k, Z\rangle$ and $\varepsilon_i = 0$ or 1 $(i = 1, \ldots, k)$.

Moreover, $\ell(\alpha) = \ell(G) = \frac{2^{k+1}}{2^{k+1}}$.

Type 3. G is nilpotent of class 2. It has elementary Abelian commutator subgroup $\langle z_1, z_2\rangle$ of order 4. Its centre Z has index 2^4 in G and G/Z is an elementary Abelian 2-group, generated by x_1Z, x_2Z, a_1Z, a_2Z subject to the commutator relations

$$[x_1, x_2] = [a_1, a_2] = [a_1, x_2] = [a_2, x_1] = 1,$$

$$[a_1, x_1] = z_1, \quad [a_2, x_2] = z_2 .$$

Every such group has a $> \frac{1}{2}$-automorphism α defined by the map

$$(a\,x_1^{\varepsilon_1}x_2^{\varepsilon_2})\alpha = a^{-1}x_1^{-\varepsilon_1}x_2^{-\varepsilon_2},$$

for all $a \in A = \langle a_1, a_2, Z\rangle$ and $\varepsilon_i = 0$ or 1 $(i = 1, 2)$.

Moreover, $\ell(\alpha) = \ell(G) = \frac{9}{16}$.

(1.3.14) Comments and Examples. Note that in (1.3.13) we do not specify the orders of the x_i's and the a_i's in groups of type 2 and 3. The only condition imposed on powers of these elements is that their squares must lie in the centre Z of G, for clearly $[a_i^2, x_j] = [a_i, x_j^2] = [a_i, x_j]^2 = 1$ for all i, j. It follows immediately from the structure theorem that in a $> \frac{1}{2}$-group G of type 2 or 3 the elements of odd order form a subgroup Z_o of the centre and G splits into a direct product of Z_o and a 2-group.

The dihedral group D_n $(n \geq 3)$ of order 2n is an example of a group of type 1. The direct product of the quaternion group Q and the group D_4, with centres amalgamated, is a group of type 2. In fact any extra-special 2-group is a group of type 2 and this type is characterised by the condition $|G'| = 2$.

The most elementary example of a group of type 3 is the direct product of the quaternion group Q and the group D_4. In fact the direct

product of any two groups with a $\frac{3}{4}$-automorphism is a group of type 3.

SECTION (1.4) Groups consisting mostly of involutions

In [13] Wall classified all groups at least half of whose elements were involutions. This problem has a long history, having been considered in a series of papers by G. A. Miller [9] who finally arrived at a classification which is not too easy to follow. We obtain a solution of this problem by classifying all groups in which the identity automorphism is a $> \frac{1}{2}$-automorphism. We thus present an alternative treatment by "elementary" methods, since Professor Wall used character theory in his analysis.

Throughout this section we let G denote a non-Abelian group such that the identity automorphism, ι, is a $> \frac{1}{2}$-automorphism. Thus G has precisely $\ell(G)|G| - 1 \geq \frac{1}{2}|G|$ involutions.

(1.4.1) Groups of Type 1. Two cases arise. If A is an Abelian subgroup of maximum order in G then *either (i)* every element of A is mapped by ι onto its inverse, and so A is an elementary Abelian 2-group; *or (ii)* A is not elementary Abelian. In this case, by the proof of Theorem (1.2.2) with $\alpha = \iota$, there is an inner automorphism I_x $(x \in S_\iota)$ that inverts A elementwise. In other words, there exists an involution x such that

$$x^{-1}ax = a^{-1} \text{ for all } a \in A,$$

and so

$$(xa)^2 = 1 \text{ for all } a \in A.$$

In either case the centre Z of G is an elementary Abelian 2-group.

We now employ Theorem (1.3.13) to obtain the structure of G. In case (i) G has an elementary Abelian subgroup A of index 2 and an involution $x \notin A$ which induces by conjugation an arbitrary automorphism of order 2 in A. These groups appear in class IV of Wall's classification.

In case (ii), G has an Abelian subgroup A of index 2 and arbitrary order which is not elementary Abelian, and an involution $x \notin A$ which

induces in A the automorphism that inverts A elementwise. These groups appear in class I of Wall's classification.

Clearly in this case G may be chosen to have arbitrary even order ≥ 6.

(1.4.2) Groups of Type 2. The centre Z of G may be written as a direct product $Z = \langle z \rangle \times E$ where z generates the commutator subgroup of G, and E is an elementary Abelian 2-group (if non-trivial). Clearly E splits from G for otherwise at least half the elements of G have order > 2. So $G = G_o \times E$, where G_o is a type 2 group with centre G_o' of order 2. We show that G_o has an Abelian subgroup of maximum order that is elementary Abelian. For the square of every element of G_o is equal to z or 1 and so one of a_i, x_i, $a_i x_i$ has order 2. We select such an element for each i ($i = 1, \ldots, k$). They generate with z the required elementary Abelian subgroup.

It follows that G_o has the presentation $G_o = \langle z, x_1, \ldots, x_k, a_1, \ldots, a_k | z^2 = x_i^2 = a_i^2 = 1$, all pairs of generators commute except $[a_i, x_i] = z$ $(i = 1, \ldots, k) \rangle$. These are Walls class III groups. As he points out, they are the product of k dihedral groups of order 8 with centres amalgamated.

(1.4.3) Type 3. Here $G = G_o \times E$, where G_o is a type 3 group whose centre G_o' is a four-group. Hence G_o has order 64 and an analysis similar to the above shows that there is only one group of this type that admits ι as a $> \frac{1}{2}$-automorphism. G_o has presentation
$G_o = \langle z_1, z_2, a_1, a_2, x_1, x_2 | z_i^2 = x_i^2 = a_i^2 = 1$, all pairs of generators commute except $[a_i, x_i] = z_i$ $(i = 1, 2) \rangle$.

This is Wall's class II group: it is the direct product of two dihedral groups of order 8.

CHAPTER 2 GROUPS OF ODD ORDER

SECTION (2.1) Introduction

We next turn our attention to the case where G has odd order. Let G be a non-Abelian group and let p (odd) be the smallest prime which divides the order of G. It is known that no automorphism of G inverts more than $\frac{1}{p}$ of the elements of G. In this chapter we obtain a complete classification of groups G in which some automorphism inverts exactly $\frac{1}{p}|G|$ elements. We show that either G has an Abelian subgroup of index p and an element of order p not contained in this subgroup, or G is a direct product of a p-group of nilpotency class 2 or 3 and an Abelian p'-group. The detailed structure is given in Theorems 2.3.7, 2.4.4, and 2.5.1.

The result (Lemmata 2.2.3 and 2.2.4) that G has an automorphism inverting $\frac{1}{p}$ of its elements if and only if G has an involutory automorphism fixing exactly p elements, leads to an alternative formulation of our problem: classify all non-Abelian groups of odd order with an involutory automorphism whose fixed point group is as small as possible. Since a group of odd order is Abelian if and only if it has a fixed-point-free automorphism of order 2, we are again considering groups which are "almost" Abelian in some sense. Our problem is also a very special case of that of Kovács and Wall [6] and Ward [14] who studied the structure of odd order groups with an involutory automorphism whose fixed point group is nilpotent.

In [10] and [11] Miller considered the case where G is an odd order p-group. Some of his results are in conflict with ours and he did not obtain a classification.

There is an obvious similarity between $\frac{1}{p}$-groups and the $>\frac{1}{2}$-groups classified in Chapter 1.

SECTION (2.2) Preliminary Theorems

We begin by showing that if G belongs to G_p ($p > 2$) then $\ell(G) \leq \frac{1}{p}$. (Our attention was drawn to this result by Dr. T. J. Laffey.)

(2.2.1) Lemma: Let G be a group of odd order and let α be an automorphism of G with $\alpha^2 = 1$. Then

(i) $S_\alpha = \{g^{-1}g(\alpha) \mid g \in G\}$;

(ii) $G = S_\alpha F_\alpha$, $S_\alpha \cap F_\alpha = 1$, and $|S_\alpha| = (G : F_\alpha)$.

Proof (Gorenstein [1] 10.4) (i) Clearly $(g^{-1}(g\alpha))\alpha = (g^{-1}(g\alpha))^{-1}$. Conversely, suppose $s \in S_\alpha$, and $s^{2n+1} = 1$. Then $s = g^{-1}(g\alpha)$ where $g = s^n$.

(ii) $x^{-1}(x\alpha) = y^{-1}(y\alpha)$ if and only if $yx^{-1} \in F_\alpha$ and $S_\alpha f_i \cap S_\alpha f_j$ is empty unless $f_i = f_j$, where $f_i, f_j \in F_\alpha$.

(2.2.2) Theorem. If $G \in G_p$ and p is odd, then $\ell(G) \leq \frac{1}{p}$.

Proof. Assume $\ell(G) > \frac{1}{p}$. Let α be an automorphism with $|S_\alpha| > \frac{1}{p}|G|$. The elements of S_α generate G and so $\alpha^2 = 1$. By Lemma (2.2.1) (ii), $p(G : F_\alpha) > |G|$. Since F_α is a subgroup of G, it follows that $F_\alpha = 1$ and $S_\alpha = G$, contradicting the fact that G is non-Abelian.

We proceed to investigate the structure of groups $G \in G_p$ ($p > 2$) with $\ell(G) = \frac{1}{p}$. Our immediate aim is to show that either G has a $\frac{1}{p}$-automorphism α such that S_α is a subgroup, or G is a direct product of a p-group and an Abelian p'-group.

For the rest of this section G denotes a group in G_p ($p > 2$) with a $\frac{1}{p}$-automorphism α.

(2.2.3) Lemma. Every $\frac{1}{p}$-automorphism of G has order 2.

Proof. Let α be a $\frac{1}{p}$-automorphism. If S_α is not a subgroup then $\langle S_\alpha \rangle = G$ and clearly $\alpha^2 = 1$. Suppose that $S_\alpha = A$, a subgroup of G. Then A is Abelian and of index p in G, and so is normal in G since p is the least prime which divides the order of G. Let $G = \langle A, g \rangle$. It is sufficient to show that $g\alpha^2 = g$. Now for all $a \in A$, $gag^{-1} \in A$ and so

$$(gag^{-1})^{-1} = (gag^{-1})\alpha = (g\alpha)a^{-1}(g\alpha)^{-1}.$$

Hence $g^{-1}(g\alpha)$ centralizes A and so belongs to A, since G is non-Abelian. That is $g\alpha = ga^*$ for some $a^* \in A$, and $g\alpha^2 = (g\alpha)a^{*-1} = g$.

(2.2.4) Lemma. For every $\frac{1}{p}$-automorphism α, $|F_\alpha| = p$.

Proof. This is an immediate consequence of Lemma (2.2.1)(ii).

(2.2.5) Lemma. No element of the set $S_\alpha f$, $f \in F_\alpha$, $f \neq 1$, is inverted by α.

Proof. Suppose $s \in S_\alpha \cap S_\alpha f$. Then $s = s_1 f$ for some $s_1 \in S_\alpha$. Application of α gives $s_1 s^{-1} = s_1^{-1} s$ and hence $s^2 = s_1^2$. But $|G|$ is odd, and so $s = s_1$ and $f = 1$, a contradiction.

We now define $A(= A_\alpha)$ to be a subgroup of G of maximum order in S_α, where α is a $\frac{1}{p}$-automorphism of G. A is clearly Abelian.

(2.2.6) Lemma. Let $g \in G \setminus A$ and suppose that the set $Ag \cap S_\alpha$ is not empty. Then

$$|Ag \cap S_\alpha| = |C_A(g)| \leq \frac{1}{p}|A|.$$

Proof. By hypothesis $Ag \cap S_\alpha$ is not empty, so we may choose $s \in S_\alpha$ such that $Ag = As$. Now for $a \in A$, $(as)\alpha = (as)^{-1}$ if and only if $[a, s] = 1$. Hence $Ag \cap S_\alpha = (C_A(s))s$. But $C_A(s) = C_A(g)$, and the equality follows.

Finally, suppose $C_A(g) = A$; then $C_A(s) = A$ and so $\langle s, A \rangle \subseteq S_\alpha$. By the maximality of A, $s \in A$ and hence $g \in A$, a contradiction. Since $C_A(g)$ is a subgroup of A, the inequality follows.

(2.2.7) Theorem. (Coset decomposition of G relative to A.) Let f generate F_α. Then there exists a coset decomposition

(2.2.8) $G = A \cup Af \cup Af^2 \cup \ldots \cup Af^{p-1}$ if $(G : A) = p$;

(2.2.9) $G = A \cup Af \cup Af^2 \cup \ldots \cup Af^{p-1} \cup As_1 \cup \ldots \cup As_n$ if $(G : A) > p$, such that $s_i \in S_\alpha$ $(i = 1, \ldots, n)$. Moreover,

(i) $Af^i \cap S_\alpha$ is empty $(i = 1, \ldots, p-1)$;

(ii) $|As_j \cap S_\alpha| = |C_A(s_j)| = \frac{1}{p}|A|$ $(j = 1, \ldots, n)$.

Proof. No non-trivial element of A is fixed by α, and so we may choose distinct cosets $Af^i (i = 1, \ldots, p-1)$. Lemma 2.2.5 gives result (i). Clearly exactly $\frac{1}{p}$ of the elements of $A \cup Af \cup \ldots \cup Af^{p-1}$ are inverted by α. By Lemma 2.2.6 every other coset must have exactly $\frac{1}{p}$ of its elements in S_α.

(2.2.10) Lemma. Let B be a subgroup of maximum order in S_β, where $\beta = I_s\alpha$ for some $s \in S_\alpha$. Then $|A| = |B|$.

Proof. Clearly both s and $C_A(s)$ are contained in S_β and so is the subgroup $X = \langle C_A(s), s \rangle$. Thus $|B| \geq |X|$ and by Theorem 2.2.7, $|X| \geq |A|$.

Conversely, $\alpha = I_{s^{-1}}\beta$, where $s^{-1} \in S_\beta$ and thus by the above proof $|A| \geq |B|$, which proves the lemma.

Lemma (2.2.10) does not hold for arbitrary $\frac{1}{p}$-automorphisms α and β, as will be shown in examples 2.5.3 and 2.5.4.

(2.2.11) Theorem. For all $x \in G$, $x^p \in A$.

Proof. Suppose first that $x = as$ for some $a \in A$, $s \in S_\alpha$. The subgroup $B = \langle C_A(s), x \rangle$ is inverted elementwise by $\beta = I_a\alpha$. By Theorem (2.2.7) $|B| \geq |A|$, and so by Lemma (2.2.10), $|B| = |A|$. Hence $x^p \in C_A(s) \subset A$.

It remains to prove the result for elements $x = af$ where f is an arbitrary generator of F_α. Since $(af)^p \in A$ if and only if $(fa)^p \in A$, we may assume that $fa \in Af^r$ for some integer r. We show that $r = 1$. For $faf^{-r} \in A$ and $(faf^{-r})\alpha = fa^{-1}f^{-r} \in A$ which implies that $fa^2f^{-1} \in A$ and (since $|G|$ is odd) that $faf^{-1} \in A$.

We suppose by way of contradiction that $(a_1f)^p \notin A$ for some $a_1 \in A$. By the above, $fa_1 = a_2f$ for some $a_2 \in A$. Moreover $(a_2f)^p \notin A$, for otherwise $(fa_1)^p$ and $(a_1f)^p$ are both contained in A. Proceeding in this way we obtain a sequence of elements $a_1, \ldots, a_p$ of A such that $fa_i = a_{i+1}f$ $(i = 1, \ldots, p-1)$ and $(a_{i+1}f)^p \notin A$. But then $(a_1f)^p = a_1 a_2 \ldots a_p f^p \in A$. and this contradiction establishes the theorem.

(2.2.12) Corollary. Every p'-element of G belongs to A.

(2.2.13) Theorem. If $(G : A) > p$ then G is the direct product $P \times M$ of a Sylow p-subgroup P, with $\ell(P) = \frac{1}{p}$ and an Abelian p'-subgroup M contained in A.

Proof. For every prime divisor q of $|G|$, $q \neq p$, G has a unique Sylow q-subgroup and this belongs to A by Corollary 2.2.12. Let M denote the direct product of all such subgroups. Clearly M is Abelian and characteristic in G. We must show that M belongs to the centre of G. By hypothesis G has a coset decomposition 2.2.9 relative to A. We first show that every element of As_i centralizes M ($i = 1, \ldots, n$).

For all $m \in M$, $s_i^{-1} m s_i \in M$. Hence $(s_i^{-1} m s_i)^{-1} = (s_i^{-1} m s_i)\alpha = s_i m^{-1} s_i^{-1}$ From this it follows that s_i^2 and thus also s_i commutes with m.

To show that f commutes with m, we consider $s_1 f$. This element clearly cannot belong to a coset Af^j ($j = 0, \ldots, p-1$). Thus $s_1 f \in As_i$ for some i, and as was shown above, both s_1 and $s_1 f$ commute with m; hence so does f.

It is now clear that $G = P \times M$, and that a $\frac{1}{p}$-automorphism of G that inverts A elementwise induces a $\frac{1}{p}$- automorphism in P.

As a consequence of this theorem, in order to classify groups $G \in G_p$ with $\ell(G) = \frac{1}{p}$, it is sufficient to consider the following cases:

I. G is a p-group with a $\frac{1}{p}$-automorphism α such that $(G : A_\alpha) > p$.

II. Some Abelian subgroup of index p in G is elementwise inverted by a $\frac{1}{p}$-automorphism.

In order to show that groups satisfying condition I are divided into two distinct types we need some further analysis. For the rest of this section let G denote a p-group ($p > 2$) with a $\frac{1}{p}$-automorphism such that A ($= A_\alpha$) has index at least p^2 in G.

(2.2.14) Lemma. Let $s \in S_\alpha \setminus A$. Then $s \notin N_G(A)$.

Proof. Suppose to the contrary that $s^{-1}as \in A$ for all $a \in A$. Then $(s^{-1}as)^{-1} = (s^{-1}as)\alpha = sa^{-1}s^{-1}$, and hence s^2 and s commute with a. Thus $A \subset \langle A,s \rangle \subseteq S_\alpha$ and this contradicts the maximality of A.

(2.2.15) Lemma. Let f generate F_α. Then

(i) $N_G(A) = \langle A,f \rangle$ and $(N_G(A) : A) = p$;

(ii) $N_G(A)$ is normal in G.

Proof. (i) Consider a coset decomposition (2.2.9). By Lemma 2.2.14, no element as_i, $a \in A$ $(i = 1, \ldots, n)$ belongs to $N_G(A)$. Since G is a p-group, A is properly contained in its normalizer and the result follows.

(ii) Let $N = N_G(A)$. It is sufficient to show that $s^{-1}Ns = N$ for every $s \in S_\alpha \setminus N$. Write $A = \langle C_A(s), a \rangle$. We must show that $s^{-1}as$ and $s^{-1}fs$ belong to N. Suppose by way of contradiction that $s^{-1}as \notin N$. Then according to (2.2.9), $s^{-1}as \in As_i$ for some $s_i \in S_\alpha$, that is

$$s^{-1}as = a^r c s_i, \text{ where } c \in C_A(s) \text{ and } 0 \leq r < p.$$

Hence α inverts $c^{-1}a^{-r}s^{-1}as$ whence sa^rs commutes with a. If $r = 0$ then s^2 and hence s commutes with a, contrary to hypothesis. If $r > 0$, then, since sa^rs commutes with a^r, we obtain $(sa^r)^2 = (a^rs)^2$, whence $sa^r = a^rs$ and $as = sa$, again a contradiction.

Finally, the assumption that $s^{-1}fs \in As_i$ for some $s_i \in S_\alpha$ leads to the untenable conclusion that $x^{-1}fx = f^{-1}$ for some $x \in G$.

We are now in a position to state the various types of $\frac{1}{p}$-groups which arise and to analyse each type individually.

Type 4. G is a p-group $(p > 2)$ with a $\frac{1}{p}$-automorphism α such that $A\ (= A_\alpha)$ has index at least p^2 in G. In addition, $N_G(B)$ is Abelian for all subgroups B of maximum order in S_α.

Type 5. G is a p-group $(p > 2)$ with a $\frac{1}{p}$-automorphism α such that $A\ (= A_\alpha)$ has index at least p^2 in G. In addition, $N_G(A)$ is non-Abelian for some subgroup A of maximum order in S_α.

Type 6. Some Abelian subgroup of index p in G is elementwise inverted by a $\frac{1}{p}$-automorphism.

SECTION (2.3). Groups of Type 4

Throughout this section we let G be a group of type 4.

(2.3.1) Lemma. The subgroup F_α is contained in the centre of G.

Proof. As before suppose that F_α is generated by f. By Lemma 2.2.15, $f \in N_G(A)$; hence f commutes with every element of A. Now consider $s \in S_\alpha \backslash A$. Put $B = \langle C_A(s), s \rangle$. Then $B \subset S_\alpha$ and $|B| = |A|$. By Lemma 2.2.15 $N_G(B) = \langle B, f \rangle$, which is Abelian by hypothesis. Thus f commutes with s, and the proof is complete.

(2.3.2) Lemma. The commutator subgroup G' is equal to F_α, and so G is nilpotent of class 2.

Proof. We first show that for any $s \in S_\alpha \backslash A$, $[A, s] = F_\alpha$.

Let $A = \langle C_A(s), a \rangle$. By Lemmata 2.2.14 and 2.2.15 (i)

$$s^{-1}as = a^r cf,$$

where $c \in C_A(s)$ and f generates F_α. Applying α we get

$$sa^{-1}s^{-1} = a^{-r}c^{-1}f,$$

and hence, since f is central

$$sa^{-1}s^{-2}as = f^2 .$$

Thus $[a, s^2] \in F_\alpha$ and the result follows.

Now let s^* be an arbitrary element of S_α. By considering $A^* = \langle C_A(s^*), s^* \rangle$, which is elementwise inverted by α, we obtain $[s^*, s] \in F_\alpha$. But the elements of S_α generate G and so the lemma is proved.

In Lemma 2.2.15 (ii) we showed that N ($= N_G(A)$) is a normal subgroup of G. We now know that it contains G'. Thus by Theorem 2.2.11 the quotient group G/N is elementary Abelian.

We now examine the centralizers in A of elements in $G \backslash N$.

(2.3.3) Lemma. For elements $x, y \notin N$, $C_A(x) = C_A(y)$ if and only if $y \in Nx^t$ for some t, $0 < t < p$.

Proof. Suppose that $C_A(x) = C_A(y) = C$. Then $A = \langle C, a \rangle$ and $[a, x] = f$, $[a, y] = f^t$, where $0 < t < p$ and f generates F_α. Hence

$$[a, w] = 1, \quad \text{where } w = yx^{-t}.$$

Contradict the lemma by supposing $w \notin N$. The coset Nw contains elements inverted by α, and so there exists $a^* \in A$ and $s \in S_\alpha \backslash A$ such that $w = a^*s$. The $\frac{1}{p}$-automorphism $\beta = (I_{a^*})\alpha$ inverts w and every element of A. Thus $B = \langle A, w \rangle \subset S_\beta$. By Lemma 2.2.10, $w \in A$, a contradiction.

The converse is obvious.

(2.3.4) Corollary. Suppose the elementary Abelian group G/N is generated as a direct product by $Nx_1, \ldots, Nx_k$. Put $D = \bigcap_{i=1}^{k} C_A(x_i)$. Then A/D is also elementary Abelian of order p^k.

Proof. Since $(A : C_A(x)) = p$ for all $x \notin N$, A/D is clearly elementary Abelian of order $\leq p^k$. But, by Lemma 2.3.3, A/D must have as many distinct subgroups of index p as there are subgroups of order p in G/N. Hence (Zassenhaus [15], page 143) A/D has order p^k.

(2.3.5) Lemma. Let $x_1, \ldots, x_k$ and D be defined as in Corollary 2.3.4. Then there exist generators $Da_1, \ldots, Da_k$ of A/D such that

$$[a_i, x_j] = 1, \ i \neq j; \quad [a_i, x_i] = f, \ i = 1, \ldots, k,$$

where f generates F_α.

Proof. Put $D_i = \bigcap_{\substack{j \neq i \\ 1 \leq j \leq k}} C_A(x_j)$. Then D has index p in D_i and $D_i = \langle D, a_i \rangle$, where $a_i^p \in D$. Since $a_i \notin C_A(x_i)$, the commutator $[a_i, x_i]$ is equal to $f^{r_i} \neq 1$, where f is a fixed generator of F_α. By replacing a_i by a power of itself, if necessary, it is possible to have $r_i = 1$ for all i. It is clear that $[a_i, x_j] = 1$ when $i \neq j$.

(2.3.6) Lemma. The elements $x_1, \ldots, x_k$ introduced in Corollary 2.3.4 can be chosen to commute pairwise.

Proof. Suppose we are given $x_1, \ldots, x_k$ such that $[x_j, x_1] = f^{t_j}$ $(j = 2, \ldots, k)$. Then there exist coset representatives of G/N $x_1^* = x_1$, $x_j^* = a_1^{-t_j} x_j$ such that $[x_j^*, x_1^*] = 1$ $(j = 2, \ldots, k)$. Note that the new coset representatives satisfy the relations of Lemma 2.3.5. The proof is now easily completed by induction in the manner of Lemma 1.3.12.

We can now give the structure of groups of Type 4.

(2.3.7) Theorem. Let G be a group of type 4. Then G is nilpotent of class 2 with commutator subgroup $\langle f \rangle$ of order p. Its centre is a direct product $Z = D \times \langle f \rangle$ and has index p^{2k} in G. G/Z is elementary Abelian, generated by $Za_1, \ldots, Za_k, Zx_1, \ldots, Zx_k$ subject to the relations

$$[x_i, x_j] = [a_i, a_j] = 1 \text{ for } i, j = 1, \ldots, k,$$

$$[a_i, x_j] = 1 \ (i \neq j), \ [a_i, x_i] = f \ (i = 1, \ldots, k).$$

The pth power of x_i and of a_i $(i = 1, \ldots, k)$ lies in D. Conversely, every such group has a $\frac{1}{p}$-automorphism α, whose fixed group is $\langle f \rangle$, defined by the map

$$(af^t x_1^{q_1} \ldots x_k^{q_k})\alpha = a^{-1} f^t x_1^{-q_1} \ldots x_k^{-q_k}$$

for all $a \in \langle a_1, \ldots, a_k, D \rangle$ and $0 \leq q_i < p (i = 1, \ldots, k)$.

The simplest examples of groups of type 4 are a non-Abelian group of order p^3 and exponent p $(k = 1)$, and the central product of two such groups $(k = 2)$. In both cases $D = 1$.

It is possible to show that groups in G_p with a $\frac{1}{p}$-automorphism of type 4 are characterised by the fact that $G' = C_p$ and $G^p \cap G' = 1$.

SECTION (2.4) Groups of Type 5

In this section let A be such that N $(= N_G(A))$ is non-Abelian. By Lemma 2.2.15, $N = \langle A, f \rangle$ where f generates F_α.

(2.4.1) Lemma. Let $x \notin N$. Then $C_A(x) = C_A(f) = Z$, the centre of G.

Proof. There exists $s \in S_\alpha$ such that $x \in As$. Hence $C_A(x) = C_A(s)$. To prove the lemma we show that

$$C_A(s) = C_A(sf) = C_A(f).$$

Suppose that $a \in C_A(sf)$. Then $s^{-1}as = faf^{-1} \in A$, and a new familiar argument gives $a \in C_A(s)$, and $C_A(sf) \subseteq C_A(s)$. Now $sf \notin N$, and $C_A(sf)$ and $C_A(s)$ both have index p in A. Hence they are equal, and thus $C_A(s) = C_A(sf) = C_A(f)$.

(2.4.2.) Lemma. The centre of G/Z is $\langle Zf \rangle$.

Proof. Put $N = \langle Z, a, f \rangle$ where $a \in A$. Since N/Z has order p^2 it is Abelian and so $[a, f] \in Z$. Now consider $s \in S_\alpha \setminus N$. The subgroup $B = \langle Z, s \rangle$ is elementwise inverted by α. By Lemma (2.2.15) $N_G(B) = \langle B, f \rangle$, and by the above argument $[s, f] \in Z$. Thus $\langle Zf \rangle$ is a subgroup of the centre of G/Z. But every element of the centre of G/Z belongs to N/Z, and since for all $s \in S_\alpha \setminus N$, $[a, s] \notin Z$, we know that Za does not belong to the centre of G/Z. The lemma follows.

(2.4.3) Lemma. The index of N in G is p.

Proof. Suppose by way of contradiction that there exist $s_1, s_2 \in S_\alpha \setminus N$ with $s_2 \notin Ns_1^r$ for all r, $0 \leq r < p$. Put $K = \langle Z, f \rangle$, $N = \langle K, a \rangle$, $G_i = \langle N, s_i \rangle$ $(i = 1, 2)$. By Lemma 2.4.2, K is normal in G_i and G_i/K is Abelian of order p^2. Thus for a suitable choice of generator f of F_α

$$Z[a, s_1] = Zf \text{ and } Z[a, s_2] = Zf^r$$

for some r, $0 < r < p$. Hence we find $x = s_1^{-r}s_2 \notin N$ but $[a, x] \in Z \subset A$, and so x normalizes $\langle Z, a \rangle = A$, contradicting the fact that N is the normalizer of A.

(2.4.4) Theorem. A group G of type 5 has centre Z of index p^3 such that G/Z is non-Abelian of exponent p. Conversely, every such p-group has a $\frac{1}{p}$-automorphism.

Proof. By the results of this section a group G of type 5 has G/Z

of order p^3. Moreover G/Z is non-Abelian, and since $x^p \in C_A(x) = Z$ for all $x \in G$, the exponent of G/Z is p.

Conversely, consider a p-group G with centre Z such that G/Z has order p^3 and exponent p. Then $G = \langle Z, a, f^*, s \rangle$ where

(i) G/Z has centre of order p generated by Zf^* ;

(ii) there exist $z_1, z_2, z_3 \in Z$ such that

$$[a, s] = f^* z_1, \quad [f^*, s] = z_2, \quad [f^*, a] = z_3$$

and one of z_2 and z_3, say z_3, is not equal to the identity;

(iii) $1 = [f^{*p}, s] = [f^*, s]^p = z_2^p$ and similarly $z_3^p = 1$.

An easy calculation gives

$$[a^m, s^n] = (f^* z_1)^{mn} z_2^{m\binom{n}{2}} z_3^{n\binom{m}{2}} .$$

Hence $(f^* z_1)^p = 1$. Now write $f = f^* z_1 (z_2 z_3)^{-\frac{p+1}{2}}$.
Clearly $f^p = 1$.

We now claim that G has a $\frac{1}{p}$-automorphism that maps a to a^{-1}, s to s^{-1}, f to f, and z to z^{-1} for all $z \in Z$. To see this we note

$$[a, s] = f(z_2 z_3)^{\frac{p+1}{2}}, \quad [f, s] = z_2, \quad [f, a] = z_3,$$

and $[a^{-1}, s^{-1}] = [a^{p-1}, s^{p-1}] = f(z_2 z_3)^{\frac{p+1}{2}} z_2^{-1} z_3^{-1} = f(z_2 z_3)^{-\frac{p+1}{2}}$.

The rest of the verification is routine.

SECTION (2.5) Groups of Type 6.

Theorem (2.5.1) A group G in G_p which has an Abelian subgroup A of index p in G has a $\frac{1}{p}$-automorphism inverting A elementwise if and only if there exists $f \in G \setminus A$ such that $f^p = 1$.

Proof. Suppose that α is a $\frac{1}{p}$-automorphism such that $S_\alpha = A_\alpha = A$, a subgroup of index p in G. Then, by Lemma 2.2.4, F_α is generated by f of order p and clearly $f \notin A$.

Conversely, given $G = \langle A, f \rangle \in G_p$ with $f^p = 1$ and A an Abelian subgroup of index p in G, then A is normal in G and the map α

$$(af^i)\alpha = a^{-1}f^i,\ a \in A\ (i = 0, \ldots, p-1),$$

defines a $\frac{1}{p}$-automorphism of G which inverts the elements of A. Hence $G \in G_p$ has type 6 if and only if G has an Abelian subgroup A of index p which does not contain all the elements of order p in G.

(2.5.2) Example. There exist groups in G_p with an Abelian subgroup of index p which do not have $\frac{1}{p}$-automorphisms. This fact is illustrated by the group of order 63

$$G = \langle a, b \mid a^{21} = 1,\ b^{-1}ab = a^{16},\ b^3 = a^7 \rangle.$$

The unique subgroup $A = \langle a \rangle$ of index 3 in G contains all the elements of order 3.

There can be no overlap between groups of type 4 and type 5 since the orders of the corresponding central factor groups are different. However, the following examples show that there exist groups which are simultaneously of type 4 and type 6 and groups which are simultaneously of type 5 and type 6.

(2.5.3) Example. The non-Abelian group of order p^3 and exponent p is of type 4 and type 6.

(2.5.4) Example. Let $T = \langle z, f, s \rangle$ be the non-Abelian group of order p^3 and exponent p, where $[f, s] = z$. Let G be the split extension of T by the automorphism $z \to z$, $f \to fz^{-1}$, $s \to sf^{-1}$, that is, $G = \langle T, a \rangle$, where $a^p = 1$ and $[a, s] = f$; $[f, a] = z^{-1}$, $[a, z] = 1$.
The following maps define $\frac{1}{p}$-automorphisms of types 5 and 6 respectively.
$\alpha : a \to a^{-1}$, $s \to s^{-1}$, $f \to f$, $z \to z^{-1}$. $(A_\alpha = \langle a, z \rangle)$;
$\beta : a \to a$, $(as) \to (as)^{-1}$, $f \to f^{-1}$, $z \to z^{-1}$. $(A_\beta = \langle z, f, as \rangle)$.
Maximal subgroups of S_α and S_β are indicated. We note that
$|A_\alpha| \neq |A_\beta|$.

CHAPTER 3. GROUPS WITH $\frac{1}{2}$-AUTOMORPHISMS

SECTION (3.1) Introduction

We now analyse the case where some automorphism of G inverts exactly $\frac{1}{2}|G|$ elements. Since some Abelian groups and also some groups of types 1 and 2 will be seen to fall into this category, the above condition is not equivalent to the condition $\ell(G) = \frac{1}{2}$. If G is non-Abelian we show that either G has an Abelian subgroup of index 2 or 4 or G is nilpotent of class 2 with commutator subgroup of order 2. We note that in all cases G is soluble of solubility length at most 3.

The analysis of $\frac{1}{2}$-groups is considerably more involved than that of $> \frac{1}{2}$-groups or $\frac{1}{p}$-groups and the classification is subdivided into many different types, as detailed in the structure theorems.

SECTION (3.2) Abelian $\frac{1}{2}$-groups.

Throughout this section let G denote an Abelian group of even order.

(3.2.1.) Theorem. Let G be an Abelian group with a $\frac{1}{2}$-automorphism. Then G is not of the form $C_2 \times N$ where N has odd order. Conversely, every Abelian group of even order which is not of this form has a $\frac{1}{2}$-automorphism.

Proof. Let G be of the form $C_2 \times N$, where N is Abelian of odd order, and let α be a $\frac{1}{2}$-automorphism of G. Since in an Abelian group elements inverted by an automorphism form a subgroup, we have $S_\alpha = N$, and t, the unique involution in G, is characteristic in G and hence $(t)_\alpha = t = t^{-1}$. Thus we have shown that $t \in N$, a contradiction.

Conversely, if G is Abelian of even order and not of the form $C_2 \times N$, where N has odd order, we show that G has a $\frac{1}{2}$-automorphism. We look at two cases.

Case (i). G has more than one involution: let t_1 and t_2 be distinct involutions. Thus $t_1 t_2$ is also an involution. Let A be any subgroup of index 2 in G. If $t_1 \notin A$ and $t_2 \notin A$ then $t_1 t_2 \in A$, and hence A contains at least one involution, say t. The map $a \to a^{-1}$, $ax \to a^{-1}tx^{-1}$, for all $a \in A$, where $G = A \cup Ax$, defines a $\frac{1}{2}$-automorphism of G whose inverted set

is A.

Case (ii). G has exactly one involution t : If $t \notin A$ for any subgroup A of index 2, then $G = A \times \langle t \rangle$ where A has odd order, contrary to hypothesis. Hence $t \in A$ for some subgroup A of index 2 and again the map $a \to a^{-1}$, $ax \to a^{-1}tx^{-1}$ for all $a \in A$, where $G = A \cup Ax$, defines a $\frac{1}{2}$-automorphism of G.

For completeness of classification we call Abelian $\frac{1}{2}$-groups groups of Type 7.

SECTION (3.3) Preliminary Analysis.

For the remainder of this chapter we let G denote a non-Abelian $\frac{1}{2}$-group.

Examination of the alternating group on 4 symbols, which is a $\frac{1}{2}$-group, shows that the Abelian subgroup of maximum order, which is a four-group, is not elementwise inverted by any $\frac{1}{2}$-automorphism. Hence there can be no hope of an analogue of Corollary 1.2.3 for $\frac{1}{2}$-groups. With these facts in mind we make the following important definition .

(3.3.1) Definition. Let G be non-Abelian and let β be an automorphism of G for which $|S_\beta| = \frac{1}{2}|G|$.

Consider the set $D = \{I_s\beta \mid s \in S_\beta\}$, which by Lemma 1.2.1 is a set of $\frac{1}{2}$-automorphisms of G. Let A be a subgroup of maximum possible order which is elementwise inverted by α, as α ranges over the elements of D.

The subgroup A is obviously Abelian and plays a crucial role in the analysis of $\frac{1}{2}$-groups. We let $(G : A) = n$ and we suppose that α is a $\frac{1}{2}$-automorphism which inverts the elements of A. Firstly we look at the relatively easy case where $(G : A) = n = 2$.

(3.3.2) Theorem. (Groups of Type 8) Let G be a non-Abelian group with an Abelian subgroup A of index 2. Let $G = A \cup Ax$ and let $A^* = \{a \in A \mid x^{-1}ax = a^{-1}\}$. Then G has a $\frac{1}{2}$-automorphism which inverts the elements of A if and only if G' is a proper subgroup of A^*.

Proof. Since $G' = [A, x]$ and $x^{-1}[a, x]x = [x, a]$ for all $a \in A$, we see that G' is a subgroup of A^*.

Firstly, let α be an automorphism of G such that $S_\alpha = A$ and $S_\alpha \cap Ax$ is empty. Now $x^2 \in A$ and thus $(x^2)\alpha = x^{-2} = (x\alpha)^2$. But $(x)\alpha = a^*x^{-1}$ for some $a^*(\neq 1) \in A$, and thus $x^{-2} = (a^*x^{-1})^2$ whence $x^{-1}a^*x = a^{*-1}$. Now $(ax)\alpha = (ax)^{-1}$ if and only if $a^* = [x, a]$ and hence if α is a $\frac{1}{2}$-automorphism then there is an element $a^* \in A^* \setminus G'$.

Conversely, given $a^* \in A^* \setminus G'$ a routine calculation shows that the mapping $a \to a^{-1}$, $ax \to a^{-1}a^*x^{-1}$ is an automorphism of G whose inverted set is exactly A.

(3.3.3) Example. Let $D_n = \langle a, b \mid a^n = 1 = b^2, b^{-1}ab = a^{-1} \rangle$. If we let $A = \langle a \rangle$, we see that $A^* = A$. When n is odd we know that $G' = A^*$ and when n is even we know that G' is a proper subgroup of A. Theorem 3.3.2 now tells us that D_n has a $\frac{1}{2}$-automorphism of type 8 if and only if n is even.

Now we suppose that $(G : A) = n > 2$.

(3.3.4) Lemma. Let A be as defined in 3.3.1 and let α be a $\frac{1}{2}$-automorphism of G which inverts the elements of A. Suppose that $g \notin A$ and that the coset Ag has non-trivial intersection with S_α. Then $|Ag \cap S_\alpha| = |C_A(g)| = \frac{1}{n}|A|$, where n is an integer ≥ 2.

Proof. By hypothesis, $Ag \cap S_\alpha$ is not empty, so we may choose $s \in S_\alpha$ such that $Ag = As$. Now for $a \in A$, $(as)\alpha = (as)^{-1}$ if and only if $a^{-1}s^{-1} = s^{-1}a^{-1}$. Hence

$$Ag \cap S_\alpha = (C_A(s))s = (C_A(g))s$$

and the result follows.

Since $C_A(g)$ is a subgroup of A, we have $|C_A(g)| = \frac{1}{n}|A|$ and all that remains is to show that $n = 1$ is not possible.

For suppose that $n = 1$, then $C_A(g) = A = C_A(s)$, where $Ag = As$ and $s \in S_\alpha$. The proof is completed by observing that $\langle A, s \rangle$, which is contained in S_α, has order greater than that of A, contrary to the definition of A.

At this stage we introduce some terminology which will simplify the analysis. If for $g \notin A$, the coset Ag has theproperty that $|Ag \cap S_\alpha| = \frac{1}{n}|A|$, we say that Ag is a $\frac{1}{n}$-coset. If for $g \notin A$, $Ag \cap S_\alpha$ is empty, we say that Ag is an empty-coset.

(3.3.5) Lemma. At most one coset of A in G is an empty-coset.

Proof. Suppose that $G = A \cup Ag_1 \cup Ag_2 \cup As_2 \cup \ldots \cup As_{n-2}$ is a coset decomposition of G relative to A, where Ag_1 and Ag_2 are distinct empty-cosets and $s_i \in S_\alpha$ $(i = 2, \ldots, n-2)$. Then, by Lemma 3.3.4,

$$|S_\alpha| = |A| + \sum_{i=2}^{n-2} |C_A(s_i)|. \tag{3.3.6}$$

But Lemma 3.3.4 also tells us that $(A: C_A(s_i)) \geq 2$ and hence 3.3.6 contradicts the fact that $|S_\alpha| = \frac{1}{2}|G|$.

(3.3.7) Theorem. Let G be a non-Abelian group with a $\frac{1}{2}$-automorphism inverting the elements of A, where A is as defined in 3.3.1, and let $(G : A) = n > 2$. Then G has a coset decomposition

$$G = A \cup Ag \cup As_2 \cup \ldots \cup As_{n-1}, \ (n \geq 3) \tag{3.3.8}$$

where Ag is an empty-coset, $s_i \in S_\alpha$, $s_1 = 1$, and $(A : C_A(s_i)) = q_i = 2$, $(i = 2, \ldots, n-1)$ OR G has a coset decomposition

$$G = A \cup As_2 \cup As_3 \cup \ldots \cup As_n, \text{ with } s_i \in S_\alpha,\ s_1 = 1 \ (i = 1, \ldots, n) \tag{3.3.9}$$

and the following equality on the indices $q_i = (A : C_A(s_i))$ holds:

$$\sum_{i=2}^{n} \left(\frac{1}{2} - \frac{1}{q_i}\right) = \frac{1}{2}. \tag{3.3.10}$$

Proof. By Lemma 3.3.5 at most one coset of A in G is an empty-coset. If exactly one coset is an empty-coset, then we get the decomposition 3.3.8. Since by Lemma 3.3.4

$$\frac{1}{2}|G| = |S_\alpha| = |A| + \sum_{i=2}^{n-1} |C_A(s_i)|$$

and $(A : C_A(s_i)) \geq 2$, we must have $(A : C_A(s_i)) = 2$ $(i = 2, \ldots, n-1)$.

If every coset of A in G has non-trivial intersection with S_α, we get a coset decomposition 3.3.9. The centralizer equality 3.3.10 is now an immediate consequence of the fact that

$$|S_\alpha| = \frac{1}{2}|G| = |A| + \sum_{i=2}^{n} |C_A(s_i)|.$$

For any given value of n there is only a finite number of solutions of the Diophantine equation 3.3.10. Hence, relative to a suitable ordering of the cosets of A in G, only the following cases can arise:

$$\text{(3.3.11)}\quad \begin{array}{ll} \text{I} & n \geq 3,\ q_2 = 6,\ q_3 = 3,\ q_i = 2\ (i = 4, \ldots, n)\ ; \\ \text{II} & n \geq 3,\ q_2 = q_3 = q_4 = 3,\ q_i = 2\ (i = 5, \ldots, n)\ ; \\ \text{III} & n \geq 3,\ q_2 = q_3 = 4,\ q_i = 2\ \ (i = 4, \ldots, n). \end{array}$$

Together with 3.3.8, cases 3.3.11. I, II, and III give rise to separate categories of $\frac{1}{2}$-groups and we proceed to examine each category in turn.

To complete this section we prove a useful Lemma.

(3.3.12) Lemma. Let G be a non-Abelian $\frac{1}{2}$-group and α an automorphism which inverts the elements of A, where A is as defined in 3.3.1. If Ag is not an empty-coset and $(A : C_A(g)) = 2$, then

(i) $(ag)^2 \in A$, for all $a \in A$,

(ii) Every element of Ag normalizes A.

Proof. (i) Since Ag is not an empty-coset, we can choose $s \in S_\alpha$ such that $Ag = As$. Hence $(A : C_A(as)) = (A : C_A(g)) = 2$. Consider $A^* = \langle C_A(as), as \rangle$, for any $a \in A$. The $\frac{1}{2}$-automorphism $I_a\alpha$ inverts as and also every element of $C_A(as)$. Thus A^* is a subgroup of S_β, where $\beta = I_a\alpha$, and hence by the definition of A, $|A^*| \leq |A|$. Since $(A : C_A(as)) = 2$ we have at once that $(as)^2 \in A$ and thus the square of every element of Ag is contained in A. (ii) Since $agag$ and $g^2 \in A$, we have $(g^{-2})(gag) = g^{-1}ag \in A$, for every a in A, and hence every element of Ag normalizes A.

SECTION (3.4) The Empty-Coset Case.

In this section we examine $\frac{1}{2}$-groups G with a coset decomposition of type 3.3.8, where exactly one coset of A in G contains no elements in S_α.

(3.4.1) Theorem. Let G be a non-Abelian $\frac{1}{2}$-group and let α be a $\frac{1}{2}$-automorphism of G which inverts the elements of A, with A as in 3.3.1. If a coset of G relative to A is an empty-coset, then A is normal in G and

G/A is an elementary Abelian 2-group.

Proof. Let $G = A \cup Ag \cup As_2 \cup \ldots \cup As_{n-1}$, $n \geq 3$, $s_i \in S_\alpha$, $s_1 = 1$, and $(A : C_A(s_i)) = 2$, $i = 2, \ldots, n-1$. Assume that no element of the coset Ag is contained in S_α. By Lemma (3.3.12), $(as)^2 \in A$, for all $a \in A$, $s \in S_\alpha$.

Suppose now by way of contradiction that $g^{-1} \notin Ag$. Then $g^{-1} = as$, for some $a \in A$, $s \in S_\alpha \backslash A$. Thus

$$Ag = As^{-1}a^{-1} = Aa^{-1}s^{-1}a^{-1}.$$

But $(a^{-1}s^{-1}a^{-1})\alpha = asa = (a^{-1}s^{-1}a^{-1})^{-1}$ and hence Ag is not an empty-coset. Thus we are forced to conclude that $g^{-1} \in Ag$ and hence $g^2 \in A$, where g is an arbitrary coset representative of the empty-coset. It follows that $t^2 \in A$ for all t in G. Thus A is normal in G and G/A is an elementary Abelian 2-group.

(3.4.2) Lemma. If Ag is an empty-coset, then $(A : C_A(g)) = 1$, 2, or 4.

Proof. If $s \in S_\alpha \backslash A$, we have

$$C_A(g) = C_A(s^2g) \supseteq C_A(s) \cap C_A(sg).$$

Now, since G/A is elementary Abelian, the cosets Asg, Ag, and A are distinct and hence $(A : C_A(sg)) = 2$, by Lemma 3.3.7. Hence $(A : C_A(s) \cap C_A(sg)) = 2$ or 4. Thus $C_A(g)$ contains a subgroup of index 2 or 4 in A and hence $(A : C_A(g)) = 1$, 2 or 4.

At this stage we introduce a convenient notation to simplify the analysis. Let the elementary Abelian 2-group G/A be generated by $Ax_1, \ldots, Ax_k$, $n = 2^k = (G : A)$, $x_i \in S_\alpha$ $(i = 1, \ldots, k)$. We let Ax_1x_2 be the empty-coset. We note that every coset of A in G is α-invariant and hence α (suitably restricted) induces an automorphism on any subgroup of G which contains A.

We now consider the various possibilities $(A : C_A(x_1x_2)) = 4$, 2 and 1 in turn.

(3.4.3) Lemma. If $(A : C_A(x_1x_2)) = 4$, where Ax_1x_2 is an empty-coset, then $(G : A) = 4$.

Proof. We consider $A^* = \langle A, x_1, x_2 \rangle$. Now

$$C_A(x_1x_2) \geq C_A(x_1) \cap C_A(x_2) = Z(A^*) = Z.$$

Thus since $(A : C_A(x_1x_2)) = 4$ we have $C_A(x_1) \neq C_A(x_2)$. Let us write $C_A(x_1) = Z \cup Za_2$, $C_A(x_2) = Z \cup Za_1$, where $[a_1, x_2] = [a_2, x_1] = 1$. Now A/Z is elementary Abelian of order 4, since it has two distinct subgroups of order 2.

The relations $[a_1^2, x_1] = [a_1, x_1^2] = 1$ imply that $[a_1, x_1] \in C_A(x_1)$, and the Witt Identity $[x_1^{-1}, x_2, a_1]^{x_2} [x_2, a_1^{-1}, x_1^{-1}]^{a_1} [a_1, x_1, x_2]^{x_1^{-1}} = 1$, gives at once that $[a_1, x_1] \in C_A(x_2)$. Hence $[a_1, x_1] \in C_A(x_1) \cap C_A(x_2) = Z$. Thus $[a_1, x_1] = z_1 \in Z$, with $z_1^2 = 1$, $z_1 \neq 1$. Similarly $[a_2, x_2] = z_2 \in Z$, $z_2^2 = 1$, $z_2 \neq 1$. Now $[a_1a_2, x_1x_2] = z_1z_2 \neq 1$ since $C_A(x_1x_2) = Z$ and hence $z_1 \neq z_2$.

Now suppose that there exists $x_3 \in S_\alpha \backslash A^*$. Then, since α induces $> \frac{1}{2}$-automorphisms on the groups $\langle A, x_1, x_3 \rangle$ and $\langle A, x_2, x_3 \rangle$, these groups are both of Type 2. By the Structure Theorem 1.3.13,

$$[A, x_1] = \langle z_1 \rangle = [A, x_3] = \langle z_2 \rangle = [A, x_2],$$

contradicting the fact that $z_1 \neq z_2$.

Thus we have proved that no such x_3 can exist and hence $(G : A) = 4$.

Now the condition for an element $za_1^{\varepsilon}a_2^{\delta}x_1x_2$ to be inverted by α is $[x_1, x_2] = z_1^{\varepsilon}z_2^{\delta}$, where $z \in Z$, $x_1, x_2 \in S_\alpha$. Hence, since Ax_1x_2 is an empty-coset we have

$$[x_1, x_2] \notin \langle z_1, z_2 \rangle. \tag{3.4.4}$$

The analysis of $\frac{1}{2}$-groups with an empty-coset Ax_1x_2 for which $(A : C_A(x_1x_2)) = 4$ now subdivides into groups of three distinct types, depending on whether x_i^2 $(i = 1, 2)$ are contained in Z or not.

(3.4.5) Groups of Type 9. Let $G = \langle A, x_1, x_2 \rangle$ where Ax_1x_2 is an empty-coset, Ax_1 and Ax_2 are $\frac{1}{2}$-cosets, and $C_A(x_1x_2) = C_A(x_1) \cap C_A(x_2) = Z(G) = Z$, the centre of G. By Lemma 3.4.3 we know that $C_A(x_1) = Z \cup Za_2$, $C_A(x_2) = Z \cup Za_1$, where $[a_1, x_2] = 1 = [a_2, x_1]$, and $[a_1, x_1]$ and $[a_2, x_2]$ are distinct elements of order 2 in Z. For groups of type 9, we assume that $x_1^2 \in Z$ and $x_2^2 \in Z$.

Now $(x_1x_2)^2 \in C_A(x_1x_2) = Z$. It follows that $[x_1, x_2] = z_{12} \in Z$, and since $[x_1^2, x_2] = 1$, z_{12} has order 2. By 3.4.4, G' is elementary Abelian of order 8 and is contained in the centre of G. The group G/Z is elementary Abelian of order 16.

We summarise our findings in the following Structure Theorem.

(3.4.6) Theorem. Let G be a non-Abelian $\frac{1}{2}$-group, Ax_1x_2 an empty-coset for which $(A : C_A(x_1x_2)) = 4$ and suppose that x_1^2 and x_2^2 are both contained in $C_A(x_1x_2) = C_A(x_1) \cap C_A(x_2) = Z$, the centre of G, with A as in (3.3.1). Then $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4. G is nilpotent of class 2 with elementary Abelian commutator subgroup $\langle z_1, z_2, z_{12} \rangle$ of order 8. $G/Z = \langle Za_1, Za_2, Zx_1, Zx_2 \rangle$ is elementary Abelian of order 16, and the following commutator relations hold:

$$[a_1, a_2] = [a_1, x_2] = [a_2, x_1] = 1; \quad [a_i, x_i] = z_i \ (i = 1, 2) \text{ and } [x_1, x_2] = z_{12}.$$

Conversely, every such group has a $\frac{1}{2}$-automorphism α defined by

$$(za_1^{\varepsilon_1}a_2^{\varepsilon_2}x_1^{\delta_1}x_2^{\delta_2})\alpha = z^{-1}a_1^{-\varepsilon_1}a_2^{-\varepsilon_2}x_1^{-\delta_1}x_2^{-\delta_2},$$

for all $z \in Z$, $\varepsilon_i = 0, 1$, $\delta_i = 0, 1$, $(i = 1, 2)$.

(3.4.7) Groups of Type 10. As in (3.4.5) we let $G = \langle A, x_1, x_2 \rangle$, where Ax_1x_2 is an empty-coset, Ax_1 and Ax_2 are $\frac{1}{2}$-cosets, and $C_A(x_1x_2) = C_A(x_1) \cap C_A(x_2) = Z(G) = Z$, the centre of G. In addition $A/Z = \langle a_1Z, a_2Z \rangle$ is elementary Abelian of order 4 and $(A : C_A(x_1x_2)) = 4$. Again $[a_1, x_2] = [a_2, x_1] = 1$ and $[a_1, x_1]$ and $[a_2, x_2]$ are distinct elements of order 2 in Z. For groups of type 10 we assume that exactly one of the two elements x_1^2 and x_2^2 (x_1^2, say) is contained in Z.

Since $x_1^2 \in Z$, $x_2^2 \in C_A(x_2) \setminus Z$, we have $x_1^2 = z_3$ and $x_2^2 = a_1z_4$. Since $(x_1x_2)^2 \in Z$ it follows that $[x_1, x_2] = a_1z_{12}$, with $z_{12} \in Z$. The relation $[x_1^2, x_2] = 1$ now gives $(a_1z_{12})^2 = z_1$, and thus $G' = \langle z_2, a_1z_{12} \rangle$ is isomorphic to $C_2 \times C_4$. We can now give a structure theorem to summarise our findings.

(3.4.8) Theorem. Let G be a non-Abelian $\frac{1}{2}$-group, Ax_1x_2 an empty-coset for which $(A : C_A(x_1x_2)) = 4$ and suppose that $x_1^2 \in C_A(x_1x_2) = Z$ but $x_2^2 \notin Z$, with A as in 3.3.1. Then $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4 and $A/Z = \langle Za_1, Za_2 \rangle$ is also elementary Abelian of order 4. G has Abelian commutator subgroup $\langle z_2, a_1z_{12} \rangle$ which is isomorphic to $C_2 \times C_4$. $G/Z = \langle Za_2, Zx_1, Zx_2 \rangle$ is isomorphic to $D_4 \times C_2$, and the following commutator relations hold:

$[a_1, a_2] = [a_1, x_2] = [a_2, x_1] = 1$, $[a_i, x_i] = z_i$ and $[x_1, x_2] = a_1z_{12}$, where z_i has order 2 in Z and $(a_1z_{12})^2 = z_1$ $(i = 1, 2)$, and $z_{12} \in Z$.

Conversely, any such group has a $\frac{1}{2}$-automorphism α defined by

$$(za_1^{\epsilon_1}a_2^{\epsilon_2}x_1^{\delta_1}x_2^{\delta_2})\alpha = z^{-1}a_1^{-\epsilon_1}a_2^{-\epsilon_2}x_1^{-\delta_1}x_2^{-\delta_2}$$

for all $z \in Z$, $\epsilon_i, \delta_i = 0, 1$, $(i = 1, 2)$.

(3.4.9) Groups of type 11. Again we let $G = \langle A, x_1, x_2 \rangle$, where Ax_1x_2 is an empty-coset, Ax_1 and Ax_2 are $\frac{1}{2}$-cosets, and $C_A(x_1x_2) = C_A(x_1) \cap C_A(x_2) = Z(G) = Z$, the centre of G. In addition $A/Z = \langle Za_1, Za_2 \rangle$ is elementary Abelian of order 4 and $(A : C_A(x_1x_2)) = 4$. Again $[a_1, x_2] = [a_2, x_1] = 1$, and $[a_1, x_1]$ and $[a_2, x_2]$ are distinct elements of order 2 in Z. For groups of type 11 we assume that neither of the elements x_1^2, x_2^2 is contained in Z.

Since $x_i^2 \in C_A(x_i) \setminus Z$ $(i = 1, 2)$, we have $x_1^2 = a_2z_3$ and $x_2^2 = a_1z_4$. Now it follows that $[x_1, x_2] = a_1a_2z_{12}$, with $z_{12} \in Z$. By expressing the commutator $[x_1, x_2^2]$ in two different ways we find $(a_1a_2z_{12})^2 = z_1z_2$. Thus $G' = \langle z_1, a_1a_2z_{12} \rangle$ is isomorphic to $C_2 \times C_4$.

Finally, we give another structure theorem.

(3.4.10) Theorem. Let G be a non-Abelian $\frac{1}{2}$-group, Ax_1x_2 an empty-coset for which $(A : C_A(x_1x_2)) = 4$ and suppose that $x_1^2, x_2^2 \notin C_A(x_1x_2) = Z$, the centr with A as in 3.3.1. Then $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4 and $A/Z = \langle Za_1, Za_2 \rangle$ is also elementary Abelian of order 4. G has

Abelian commutator subgroup $\langle z_1, a_1a_2z_{12}\rangle$ which is isomorphic to $C_2 \times C_4$. $G/Z = \langle Zx_1, Zx_2\rangle$ is isomorphic to the group $\langle \ell, m \mid \ell^4 = 1 = m^4, [\ell, m] = \ell^2m^2, [x,y,t] = 1$ for all $x,y,t\rangle$ and the following commutator relations hold:

$[a_1, a_2] = [a_1, x_2] = [a_2, x_1] = 1$, $[a_i, x_i] = z_i$ and $[x_1, x_2] = a_1a_2z_{12}$, where z_i has order 2 in Z and $(a_1a_2z_{12})^2 = z_1z_2$ $(i = 1, 2)$ and $z_{12} \in Z$.

Conversely, any such group has a $\frac{1}{2}$-automorphism α defined by

$$(za_1^{\varepsilon_1}a_2^{\varepsilon_2}x_1^{\delta_1}x_2^{\delta_2})\alpha = z^{-1}a_1^{-\varepsilon_1}a_2^{-\varepsilon_2}x_1^{-\delta_1}x_2^{-\delta_2},$$

for all $z \in Z$, $\varepsilon_i, \delta_i = 0, 1$, $(i = 1, 2)$.

We next turn our attention to the case where Ax_1x_2 is an empty-coset for which $(A : C_A(x_1x_2)) = 2$, where Ax_1 and Ax_2 are $\frac{1}{2}$-cosets.

(3.4.11) Lemma. If $(A : C_A(x_1x_2)) = 2$, where Ax_1x_2 is an empty-coset, then G/A is elementary Abelian of order 4.

Proof. By (3.4.1) G/A is elementary Abelian (of order >2) so we need only show that $(G : A) = 4$. We consider two cases.

(i) $C_A(x_1) \neq C_A(x_2)$. Let $A^* = \langle A, x_1, x_2\rangle$ and thus $Z(A^*) = C_A(x_1) \cap C_A(x_2) = Z$. Now $A/Z = \langle Za_1, Za_2\rangle$ is non-cyclic of order 4 since it has two distinct subgroups of index 2. Let $C_A(x_1) = Z \cup Za_2$, $C_A(x_2) = Z \cup Za_1$, where $[a_1, x_2] = [a_2, x_1] = 1$. The relations $[a_1^2, x_1] = 1 = [a_1, x_1^2]$ imply that $[a_1, x_1] \in C_A(x_1)$, and the Witt Identity

$$[x_1^{-1}, x_2, a_1]^{x_1}\,[x_2, a_1^{-1}, x_2^{-1}]^{a_1}\,[a_1, x_1, x_2]^{x_1^{-1}} = 1$$

implies that $[a_1, x_1] \in C_A(x_2)$. Hence $[a_1, x_1] = z_1$ of order 2 in Z and similarly $[a_2, x_2] = z_2$ of order 2 in Z. Now $C_A(x_1x_2) = \langle Z, a_1a_2\rangle$ and thus it follows that $[a_1a_2, x_1x_2] = 1 = z_1z_2$, whence $z_1 = z_2 = z$.

Let α be a $\frac{1}{2}$-automorphism of G which inverts the elements of A. It is clear that α induces a $\frac{1}{2}$-automorphism on A^*. The condition for an element of Ax_1x_2 to be inverted by α is $(a_1^{\gamma}a_2^{\delta}x_1x_2)\alpha = (a_1^{\gamma}a_2^{\delta}x_1x_2)^{-1}$ and an easy calculation gives $[x_1, x_2] = z^{\gamma+\delta}$. Hence, since Ax_1x_2 is an

empty-coset we have

(3.4.12) $$[x_1, x_2] \notin \langle z \rangle .$$

Now suppose by way of contradiction that there exists $x_3 \in S_\alpha \backslash A^*$ and assume for convenience that x_1 and x_2 are both in S_α. Clearly α induces $> \frac{1}{2}$-automorphisms on the groups $\langle A, x_1, x_3 \rangle$ and $\langle A, x_2, x_3 \rangle$ and these groups are both of type 2. By Theorem (1.3.13) we have $[A, x_1] = [A, x_3] = \langle z \rangle = [A, x_2]$, and the elements $[x_1, x_3]$ and $[x_2, x_3]$ are both in $\langle z \rangle$. In addition $A = C_A(x_3) \cup a_3 C_A(x_3)$, with $[a_3, x_3]$, $[a_3, x_1]$, and $[a_3, x_2]$ all contained in $\langle z \rangle$.

Since G/A is elementary Abelian $Ax_1x_2x_3 \neq Ax_1x_2$ and hence $Ax_1x_2x_3$ is a $\frac{1}{2}$-coset. It follows that $(a_1^{\beta} a_2^{\gamma} a_3^{\delta} x_1x_2x_3)\alpha = (a_1^{\beta} a_2^{\gamma} a_3^{\delta} x_1x_2x_3)^{-1}$ for some β, γ, and δ. The commutator relations now give easily that $[x_1, x_2] \in \langle z \rangle$, contradicting 3.4.12.

(ii) $C_A(x_1) = C_A(x_2) = C_A(x_1x_2)$. Letting $A^* = \langle A, x_1, x_2 \rangle$ we have $C_A(x_1) = Z(A^*) = Z$. Thus $A = Z \cup aZ$, with $[a, x_i] = z_i$ of order 2 in Z $(i = 1, 2)$. Since $[a, x_1x_2] \neq 1$ we have $z_1 \neq z_2$. Again suppose that there exists $x_3 \in S_\alpha \backslash A^*$. It is clear that α induces $> \frac{1}{2}$-automorphisms on the groups $\langle A, x_1, x_3 \rangle$ and $\langle A, x_2, x_3 \rangle$ and hence these groups are both of type 2. Theorem 1.3.13 now tells us that

$$[A, x_1] = \langle z_1 \rangle = [A, x_3] = [A, x_2] = \langle z_2 \rangle$$ and this contradiction establishes the lemma that $(G : A) = 4$ in all cases.

We now consider in detail the case where $(A : C_A(x_1x_2)) = 2$ and $C_A(x_1) \neq C_A(x_2)$.

(3.4.13) Lemma. $(x_1x_2)^2 \in C_A(x_1) \cap C_A(x_2) = Z$, the centre of G.

Proof. Since G/A is an elementary Abelian 2-group, $(x_1x_2)^2$ is contained in A. Hence $(x_1x_2)^2\alpha = (x_1x_2)^{-2}$, and assuming that x_1 and x_2 are in S_α, an easy calculation gives $(x_2x_1)^2 = (x_1x_2)^2$. It follows that $[x_i, (x_1x_2)^2] = 1$ for $i = (1, 2)$ and hence $(x_1x_2)^2 \in Z$.

The analysis now subdivides into three cases depending on whether the elements x_1^2 and x_2^2 lie in Z or not.

(3.4.14) Groups of type 12. For this type we assume that $x_1^2 \in Z$ and $x_2^2 \in Z$. By Lemma (3.4.13), $(x_1x_2)^2 \in Z$ and hence $[x_1, x_2] = z_{12}$ of order 2 in Z. By the proof of 3.4.11, $G' = \langle z, z_{12} \rangle$ is elementary-Abelian of order 4 and contained in the centre of G. $G/Z = \langle Za_1, Za_2, Zx_1, Zx_2 \rangle$ is elementary Abelian of order 16. This completes the analysis of groups of type 12 and we give a structure theorem.

(3.4.15) Theorem. Let G be a non-Abelian $\frac{1}{2}$-group, Ax_1x_2 an empty-coset for which $(A : C_A(x_1x_2)) = 2$, $C_A(x_1) \neq C_A(x_2)$, and suppose that the elements x_1^2 and x_2^2 are both contained in Z, the centre of G, with A as in 3.3.1. Then $G/A = \langle Ax_1, Ax_2 \rangle$ and $A/Z = \langle Za_1, Za_2 \rangle$ are both elementary Abelian of order 4. G is nilpotent of class 2 with elementary Abelian commutator subgroup $\langle z, z_{12} \rangle$ of order 4. $G/Z = \langle Za_1, Za_2, Zx_1, Zx_2 \rangle$ is elementary Abelian of order 16 and the following commutator relations hold: $[a_1, a_2] = [a_1, x_2] = [a_2, x_1] = 1$; $[a_i, x_i] = z$ and $[x_1, x_2] = z_{12}$.

Conversely, any such group has a $\frac{1}{2}$-automorphism α defined by

$$(z^* a_1^{\varepsilon_1} a_2^{\varepsilon_2} x_1^{\delta_1} x_2^{\delta_2})\alpha = z^{*-1} a_1^{-\varepsilon_1} a_2^{-\varepsilon_2} x_1^{-\delta_1} x_2^{-\delta_2}$$

for all $z^* \in Z$, $\varepsilon_i, \delta_i = 0$ or 1 $(i = 1, 2)$.

(3.4.16) Groups of type 13. For this type we assume that exactly one of the elements x_1^2, x_2^2 (x_1^2, say) is contained in Z. By Lemma 3.4.13, $(x_1x_2)^2 \in Z$ and hence $[x_1, x_2] = a_1z_{12}$, since $x_2^2 \in a_1Z$. The relation $[x_1^2, x_2] = 1$ implies that $(a_1z_{12})^2 = z$, where $[a_1, x_1] = [a_2, x_2] = z$. Thus $G' = \langle a_1z_{12} \rangle$ is cyclic of order 4. $G/Z = \langle Zx_1, x_2Z, a_2Z \rangle$ is isomorphic to $D_4 \times C_2$.

(3.4.17) Theorem. Let G be a non-Abelian $\frac{1}{2}$-group, Ax_1x_2 an empty-coset for which $(A : C_A(x_1x_2)) = 2$, $C_A(x_1) \neq C_A(x_2)$ and suppose that $x_1^2 \in Z$, $x_2^2 \notin Z$ where Z is the centre of G, with A as in 3.3.1. Then $G/A = \langle Ax_1, Ax_2 \rangle$ and $A/Z = \langle Za_1, Za_2 \rangle$ are both elementary Abelian of order 4. G has Abelian commutator subgroup $\langle a_1z_{12} \rangle$ which is cyclic of order 4. $G/Z = \langle Zx_1, x_2Z, a_2Z \rangle$ is isomorphic to $D_4 \times C_2$ and the

following commutator relations hold:

$[a_1, a_2] = [a_1, x_2] = [a_2, x_1] = 1$; $[a_i, x_i] = z$ of order 2 in Z $(i = 1, 2)$;
$[x_1, x_2] = a_1 z_{12}$, where $z_{12} \in Z$ and $(a_1 z_{12})^2 = z$.

Conversely, any such group has a $\frac{1}{2}$-automorphism α defined by

$$(z^* a_1^{\varepsilon_1} a_2^{\varepsilon_2} x_1^{\delta_1} x_2^{\delta_2})\alpha = z^{*-1} a_1^{-\varepsilon_1} a_2^{-\varepsilon_2} x_1^{-\delta_1} x_2^{-\delta_2},$$

for all $z^* \in Z$, $\varepsilon_i, \delta_i = 0$ or 1 $(i = 1, 2)$.

(3.4.18) Groups of type 14. For this type we assume that neither of the elements x_1^2, x_2^2 is contained in Z, the centre of G. Hence $x_1^2 \in Za_2$ and $x_2^2 \in Za_1$. By Lemma 3.4.13, $(x_1x_2)^2 \in Z$ and hence $[x_1, x_2] = a_1a_2z_{12}$, with $z_{12} \in Z$. The relation $[x_1, x_2^2] = z$ gives $(a_1a_2z_{12})^2 = 1$. Hence $G' = \langle z, a_1a_2z_{12} \rangle$ is elementary Abelian of order 4. $G/Z = \langle Zx_1, Zx_2 \rangle$, with $x_1^4, x_2^4 \in Z$ and $[x_1, x_2] \in Zx_1^2x_2^2$. Once again we give a structure theorem.

(3.4.19) Theorem. Let G be a non-Abelian $\frac{1}{2}$-group, Ax_1x_2 an empty-coset for which $(A : C_A(x_1x_2)) = 2$, $C_A(x_1) \neq C_A(x_2)$ and suppose that $x_1^2 \in Za_2$, $x_2^2 \in Za_1$, with A as in 3.3.1. Then $G/A = \langle Ax_1, Ax_2 \rangle$ and $A/Z = \langle Za_1, Za_2 \rangle$ are both elementary Abelian of order 4. G has commutator subgroup $\langle z, a_1a_2z_{12} \rangle$ which is elementary Abelian of order 4. $G/Z = \langle Zx_1, Zx_2 \rangle$, where x_1 and x_2 have order 4 (mod. Z) and $[x_1, x_2] \in Zx_1^2x_2^2$. Moreover, the following commutator relations hold:
$[a_1, a_2] = [a_1, x_2] = [a_2, x_1] = 1$; $[a_i, x_i] = z$ of order 2 in Z, for $i = 1, 2$;
$[x_1, x_2] = a_1a_2z_{12}$;

Conversely, any such group has a $\frac{1}{2}$-automorphism α defined by

$$(z^* a_1^{\varepsilon_1} a_2^{\varepsilon_2} x_1^{\delta_1} x_2^{\delta_2})\alpha = z^{*-1} a_1^{-\varepsilon_1} a_2^{-\varepsilon_2} x_1^{-\delta_1} x_2^{-\delta_2}, \text{ for all}$$

$z^* \in Z$, $\varepsilon_i, \delta_i = 0$ or 1 $i = (1, 2)$.

To complete our analysis of groups with an empty-coset Ax_1x_2 for which $(A : C_A(x_1x_2)) = 2$, we turn to the case $C_A(x_1) = C_A(x_2) = C_A(x_1x_2)$.

(3.4.20) Groups of type 15. By Lemma 3.4.11, $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4 and thus $C_A(x_1) = C_A(x_2) = C_A(x_1x_2) = Z$, the centre of G. Let $A = Z \cup Za$. Part (ii) of the proof of Lemma 3.4.11

tells us that $[a, x_1] = z_1$ and $[a, x_2] = z_2$ are distinct elements of order 2 in Z.

Now the condition that an element of Ax_1x_2 be inverted by a $\frac{1}{2}$-automorphism α is $(a^i x_1 x_2)\alpha = (a^i x_1 x_2)^{-1}$. If we assume that both x_1 and x_2 belong to S_α, a little calculation shows that this condition reduces to $[x_1, x_2] \in \langle z_1 z_2 \rangle$. Since Ax_1x_2 is an empty-coset, we have

$$[x_1, x_2] \notin \langle z_1 z_2 \rangle .$$

Because the elements x_1^2, x_2^2, and $(x_1x_2)^2$ are all contained in Z it follows that $[x_1, x_2] = z_{12}$ is contained in Z. Moreover, the relation $[x_1^2, x_2] = 1$ tells us that z_{12} has order 2.

Hence G has elementary Abelian commutator subgroup $\langle z_1, z_2, z_{12} \rangle$ of order 4 or 8, depending on whether z_{12} is equal to one of the elements z_1, z_2 or not. $G/Z = \langle Za, Zx_1, Zx_2 \rangle$ is elementary Abelian of order 8.

(3.4.21) Theorem. Let G be a non-Abelian $\frac{1}{2}$-group, Ax_1x_2 an empty-coset for which $(A : C_A(x_1x_2)) = 2$, $C_A(x_1) = C_A(x_2) = Z$ the centre of G, with A as in 3.3.1. Then $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4 and $A/Z = \langle Za \rangle$ has order 2. G is nilpotent of class 2, with commutator subgroup $\langle z_1, z_2, z_{12} \rangle$ elementary Abelian of order 4 or 8, depending on whether z_{12} is equal to one of the elements z_1, z_2 or not. $G/Z = \langle Za, Zx_1, Zx_2 \rangle$ is elementary Abelian of order 8 and the following commutator relations hold:

$$[a, x_1] = z_1, \ [a, x_2] = z_2, \ [x_1, x_2] = z_{12}.$$

Conversely, any such group has a $\frac{1}{2}$-automorphism α defined by

$$(za^i x_1^{\varepsilon_1} x_2^{\varepsilon_2})\alpha = z^{-1} a^{-i} x_1^{-\varepsilon_1} x_2^{-\varepsilon_2},$$

for all $z \in Z$, $\varepsilon_j = 0, 1$, $i = 0, 1$, $j = 1, 2$.

To complete this section we must consider the case where Ax_1x_2 is an empty-coset for which $A = C_A(x_1x_2)$.

(3.4.22) Lemma. Let G be a non-Abelian $\frac{1}{2}$-group for which Ax_1x_2 is an empty-coset with $(A : C_A(x_1x_2)) = 1$ and suppose that $(G : A) > 4$. Then $|G'| = 2$.

Proof. If $C_A(x_1) \neq C_A(x_2)$ we can find an element of A which commutes with x_1 and x_1x_2 but not with x_2. This contradiction shows that $C_A(x_1) = C_A(x_2) = Z(\langle A, x_1, x_2\rangle) = Z$. Let $A = Z \cup Za$ and as before $[a, x_i] = z_i$ of order 2 in Z (i = 1, 2). Now $[a, x_1x_2] = z_1z_2 = 1$ and hence $z_1 = z_2 = z$.

Since $(G : A) > 4$ there exists $x_3 \in S_\alpha \setminus \langle A, x_1, x_2\rangle$. It is clear that the groups $\langle A, x_1, x_3\rangle$ and $\langle A, x_2, x_3\rangle$ are both of type 2 and by theorem 1.3.13 we have

$$[A, x_1] = [A, x_3] = [A, x_2] = \langle z\rangle .$$

In addition, $[x_1, x_3]$ and $[x_2, x_3]$ are both contained in $\langle z\rangle$.

Now, since Ax_1x_2 is an empty-coset, choosing x_1 and x_2 to lie in S_α, we have $[x_1, x_2] \neq 1$. By hypothesis, the coset $Ax_1x_2x_3$ is a $\frac{1}{2}$-coset and a simple calculation gives $[x_1, x_2] \in \langle z\rangle$. Since $[x_1, x_2] \neq 1$, we have $[x_1, x_2] = z$ and thus any commutator in G is 1 or z.

If we now drop the restriction that $(G : A) > 4$ we are left with the following possibilities.

(i) $(G : A) \geq 4$ and $|G'| = 2$;

(ii) $(G : A) = 4$ and $|G'| > 2$.

Consider first the case where $(G : A) \geq 4$ and $G' = \langle z\rangle$, where z has order 2 and is contained in Z, the centre of G. Since $[c^2, d] = [c, d]^2 = 1$ for all $c, d \in G$ we see that G/Z is an elementary Abelian 2-group. By 3.4.1, $G/A = \langle Ax_1, Ax_2, \ldots, Ax_k\rangle$ is elementary Abelian of order 2^k. Let $A = C_A(x_i) \cup C_A(x_i)a$ for i = 1, 2, and let $A = C_A(x_i) \cup C_A(x_i)a_i$, for $3 \leq i \leq k$. If we write $\langle A, x_1x_2\rangle = B$, we shall find that the structure of G can be more easily obtained with the help of B.

By Lemma 3.4.22, $[a, x_1] = [a, x_2] = [x_1, x_2] = z$, of order 2 in Z, the centre of G. Thus $[ax_1x_2, x_1] = 1 = [ax_1x_2, x_2]$, and hence the centre of $\langle A, x_1, x_2\rangle$ is $C_A(x_1) \cup C_A(x_1)a\,x_1x_2$. Now consider $x_3 \in S_\alpha \setminus \langle A, x_1, x_2\rangle$, with $A = C_A(x_3) \cup C_A(x_3)a_3$. Since $\langle A, x_1, x_3\rangle$ has type 2, $C_A(x_1) \neq C_A(x_3)$ and it follows that we can choose a_3 such that $[a_3, x_1] = [a_3, x_2] = 1$ and

$[a_3, x_3] = z$. If $[x_i, x_3] = z$ then $[a_3x_i, x_3] = 1$ and hence we may choose the coset representatives x_1 and x_2 to commute with x_3. It is now clear that $C_B(x_3) = C_A(x_3) \cup C_A(x_3)ax_1x_2$, and that the centre Z^* of the group $\langle A, x_1, x_2, x_3\rangle = \langle B, x_1, x_3\rangle$ is $(C_A(x_1) \cup C_A(x_1)ax_1x_2) \cap (C_A(x_3) \cup C_A(x_3)ax_1x_2)$, with $B/Z^* = \langle Z^*a, Z^*a_3\rangle$ elementary Abelian of order 4.

An obvious argument by induction now gives us the following structure theorem.

(3.4.23) Theorem. (Groups of type 16). Let G be a non-Abelian $\frac{1}{2}$-group, Ax_1x_2 an empty-coset for which $(A : C_A(x_1x_2)) = 1$ and suppose that $|G'| = 2$, with A as in 3.3.1. Then G is nilpotent of class 2 with commutator subgroup $\langle z\rangle$ of order 2. $G/A = \langle Ax_1, Ax_2, \ldots, Ax_k\rangle$ is elementary Abelian of order 2^k and $G/B = \langle Bx_1, Bx_3, \ldots, Bx_k\rangle$ is elementary Abelian of order 2^{k-1}, where $B = \langle A, x_1x_2\rangle$. If $Z_1 = C_A(x_1) \cap C_A(x_3) \cap \ldots \cap C_A(x_k)$, then Z, the centre of G, is given by $Z = Z_1 \cup Z_1ax_1x_2$, where $A = C_A(x_1) \cup C_A(x_1)a$. $B/Z = \langle Za, Za_3, \ldots, Za_k\rangle$ is elementary Abelian of order 2^{k-1}. $G/Z = \langle Za, Za_3, \ldots, Za_k, Zx_1, Zx_3, \ldots, Zx_k\rangle$ is elementary Abelian of order 2^{2k-2} and the following commutator relations hold:

$[x_i, x_j] = [a_i, a_j] = 1$, $1 \leq i, j \leq k$, except that

$[x_1, x_2] = z$; $[a_i, x_j] = 1$, $i \neq j$, $[a_i, x_i] = z$, $3 \leq i \leq k$;

$[a, x_i] = 1$ $i \neq 1, 2$; $[a, x_1] = [a, x_2] = z$.

Conversely, any such group has a $\frac{1}{2}$-automorphism α defined by

$$(a^*x_1^{\varepsilon_1}x_2^{\varepsilon_2}x_3^{\varepsilon_3}\ldots x_k^{\varepsilon_k})\alpha = a^{*-1}x_1^{-\varepsilon_1}x_2^{-\varepsilon_2}x_3^{-\varepsilon_3}\ldots x_k^{-\varepsilon_k}$$

for all $a^* \in A$, $\varepsilon_i = 0, 1$, $1 \leq i \leq k$,

It will be noticed that groups of type 2 are identical with groups of type 16, where the subgroup A of theorem 1.3.13 is replaced by the subgroup B of theorem 3.4.23.

All that now remains is to consider the case where $(G : A) = 4$ and $|G'| > 2$. We omit the now familiar analysis and state the structure theorem.

(3.4.24) Theorem (Groups of type 17). Let G be a non-Abelian $\frac{1}{2}$-group, Ax_1x_2 an empty-coset for which $(A : C_A(x_1x_2)) = 1$, with A as in 3.3.1, and suppose that $|G'| > 2$. Then G is nilpotent of class 2 with commutator subgroup $G' = \langle z, z_{12} \rangle$ elementary Abelian of order 4. $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4 and $A/Z = \langle aZ \rangle$ has order 2, where $C_A(x_1) = C_A(x_2) = Z$, the centre of G. $G/Z = \langle Za, Zx_1, Zx_2 \rangle$ is elementary Abelian of order 8 and the following commutator relations hold:

$$[a, x_1] = [a, x_2] = z; \quad [x_1, x_2] = z_{12}.$$

Conversely, any such group has a $\frac{1}{2}$-automorphism α defined by

$$(z^* a^{\varepsilon} x_1^{\varepsilon_1} x_2^{\varepsilon_2})\alpha = z^{*-1} a^{-\varepsilon} x_1^{-\varepsilon_1} x_2^{-\varepsilon_2},$$

for all $z^* \in Z$, $\varepsilon = 0, 1$, $\varepsilon_i = 0, 1$ $(i = 1, 2)$.

SECTION (3.5) The $\frac{1}{6}$-Coset Case.

We now turn our attention to condition 3.3.11.I and throughout this section G will denote a non-Abelian $\frac{1}{2}$-group for which A (as defined in 3.3.1) gives rise to a $\frac{1}{6}$-coset and a $\frac{1}{3}$-coset.

(3.5.1) Lemma. The subgroup A is normal in G and G/A is an elementary Abelian 2-group.

Proof. If $(A : C_A(x)) = 2$, it follows from lemma 3.3.12 that $(ax)^2$ belongs to A for all a in A. Assume therefore, by way of contradiction, that $(A : C_A(x)) = 6$ but $(ax)^2 \notin A$, for some $a \in A$. Thus $A(ax)^2 \neq A$ and hence the cosets Ax and $Ax^{-1}a^{-1}$ are distinct. But $C_A(x) = C_A(x^{-1}) = C_A(x^{-1}a^{-1})$ and thus at least two cosets of A in G are $\frac{1}{6}$-cosets, contradicting condition 3.3.11. I. Hence $(ax)^2 \in A$ for all a in A and we obtain a similar result if we assume that $(A : C_A(x)) = 3$. Thus $(ax)^2 \in A$ for every $a \in A$, $x \notin A$. Since $x^2 \in A$ and $axax \in A$ it follows that $x^{-1}ax \in A$, for all a in A. Thus A is normal in G and G/A is an elementary Abelian 2-group.

(3.5.2) Lemma. The index of A in G is 4.

Proof. By lemma 3.5.1, $(G : A)$ is a multiple of 4 and hence at least one coset of A in G, Ax_1 say, is a $\frac{1}{2}$-coset. Let Ax_2 be a $\frac{1}{3}$-coset and assume,

without loss of generality, that x_1 and x_2 both belong to S_α, where α is a $\frac{1}{2}$-automorphism of G which inverts the elements of A. Then

$$C_A(x_2) = C_A(x_1^2 x_2) \geq C_A(x_1) \cap C_A(x_1 x_2).$$

where $(A : C_A(x_1x_2)) = 2$, 3, or 6. Now, since G/A is elementary Abelian, the cosets Ax_1, Ax_2, and Ax_1x_2 are distinct and hence $(A : C_A(x_1x_2)) \neq 3$, since there is a unique $\frac{1}{3}$-coset of A in G. The possibility $(A : C_A(x_1x_2) = 2$ is also ruled out because $C_A(x_2)$, a subgroup of index 3 in A, cannot contain a subgroup of index 2 or 4 in A. Hence $(A : C_A(x_1x_2)) = 6$.

Suppose now that there exists $x_3 \notin \langle A, x_1, x_2 \rangle$. Then $(A : C_A(x_3)) = 2$ and by an argument similar to the above $(A : C_A(x_3x_2)) = 6$. Since there is a unique $\frac{1}{6}$-coset of A in G, $Ax_3x_2 = Ax_1x_2$ and thus $Ax_3 = Ax_1$, a contradiction. Hence $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4.

We are now able to introduce the following notation to describe the structure of G. $G/A = \langle Ax_1, Ax_2 \rangle$, with $x_1, x_2 \in S_\alpha$. $C_A(x_1) \cap C_A(x_2) = C_A(x_1x_2) = Z$, the centre of G. $A = \langle Z, a \rangle$, where A/Z is cyclic of order 6. Hence $C_A(x_1) = Z \cup Za^2 \cup Za^4$ and $C_A(x_2) = Z \cup Za^3$.

Consider now $A^* = \langle C_A(x_1), x_1 \rangle$ which is a subgroup of maximum order in S_α, with $(G : A^*) = 4$. In addition, A^*/Z is cyclic of order 6. Now the coset A^*a is a $\frac{1}{2}$-coset and thus only the possibilities 3.3.8 and 3.3.11 I and III can arise. The possibility 3.3.11. III is ruled out by the fact that $(A^* : Z) = 6$ and hence by theorems 3.4.1 and 3.5.1, A^* is normal in G and G/A^* is elementary Abelian of order 4. Finally, it follows that since $A \cap A^* = C_A(x_1)$, $G/C_A(x_1)$ is elementary Abelian of order 8.

Thus we have proved that all commutators belong to $C_A(x_1)$ and we now proceed to investigate the possibilities for $[a, x_1]$, $[a, x_2]$, and $[x_1, x_2]$.

The relations $[a^3, x_2] = 1 = [a, x_2^2]$ imply that $[a, x_2]^3 = 1$ and $[a, x_2]^{x_2} = [a, x_2]^2$. It follows that $[a, x_2]$ is contained in $C_A(x_1) \setminus C_A(x_2)$ and thus $[a, x_2] = a^2z_2$ or a^4z_2, with $z_2 \in Z$. If $[a, x_2] = a^2z_2$, then the relation $a = x_2^{-2}ax_2^2$ implies that $a^8 \in Z$, a contradiction. Hence $[a, x_2] = a^4z_2$, with $a^{12}z_2^3 = 1$.

The possibilities for $[a, x_1]$ are z_1, a^2z_1 and a^4z_1, with $z_1 \in Z$. The relations $[a, x_1^2] = 1 = [a^2, x_1]$ easily rule out the possibilities a^2z_1 and a^4z_1 and thus $[a, x_1] = z_1$, of order 2 in Z.

Finally, we consider $[x_1, x_2]$. If $[x_1, x_2] \in a^2Z$, then $[a^4x_1, x_2] \in Z$ and if $[x_1, x_2] \in a^4Z$, then $[a^2x_1, x_2] \in Z$. Hence by a suitable adjustment of coset representatives (which does not affect the values of $[a, x_1]$ and $[a, x_2]$) we can ensure that $[x_1, x_2] = z_{12}$ lies in Z, the centre of G. Since $G/C_A(x_1)$ is an elementary Abelian 2-group, $[x_1, x_2^2] = 1$ and thus $z_{12}^2 = 1$. Now suppose that $a^ix_1x_2 \in S_\alpha$. An easy calculation gives $z_{12} = a^{4i}z_1^iz_2^i$, for some i, $0 \leq i \leq 5$. Hence $a^{4i} \in Z$, from which it follows that $i = 0$ or 3. If $i = 0$, then $[x_1, x_2] = 1$. If $i = 3$, then $z_{12} = a^{12}z_1^3z_2^3 = z_1$, and thus $[x_1, ax_2] = 1$. Hence, by a suitable adjustment of coset representative if necessary, we can always choose x_1 and x_2 to commute.

To conclude this section we collect our results in a structure theorem.

(3.5.3) Theorem (Groups of type 18). Let G be a non-Abelian $\frac{1}{2}$-group whose coset decomposition relative to A involves a $\frac{1}{6}$-coset, with A as in 3.3.1. Then $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4. The centre of G, Z, is given by $C_A(x_1) \cap C_A(x_2) = C_A(x_1x_2)$, and $A/Z = \langle Za \rangle$ is cyclic of order 6. G has Abelian commutator subgroup $G' = \langle a^4z_1z_2 \rangle$ which is cyclic of order 6. $G/Z = \langle Za, Zx_1, Zx_2 \rangle$ is isomorphic to $D_3 \times C_2 \times C_2$ subject to the relations:
$[a, x_1] = z_1$ of order 2 in Z; $[a, x_2] = a^4z_2$ of order 3 with $z_2 \in Z$;
$[x_1, x_2] = 1$.

Conversely, every such group has a $\frac{1}{2}$-automorphism α defined by

$$(za^ix_1^jx_2^k)_\alpha = z^{-1}a^{-i}x_1^{-j}x_2^{-k},$$

for all $z \in Z$, $0 \leq i \leq 5$, $0 \leq j, k \leq 1$.

(3.5.4) Examples. The direct product of the dihedral groups of orders 8 and 6 is an example of a group of type 18. In fact, the direct product

of a $\frac{3}{4}$-group and a $\frac{2}{3}$-group is always a $\frac{1}{2}$-group of type 18.

SECTION 3.6. The Case of Three $\frac{1}{3}$-cosets.

Throughout this section let G denote a non-Abelian $\frac{1}{2}$-group such that three distinct cosets of A in G are $\frac{1}{3}$-cosets.

(3.6.1) Lemma. The index of A in G is 4.

Proof. By 3.3.11. II we need only show that no coset of A in G is a $\frac{1}{2}$-coset. Assume therefore that Ax_1 is a $\frac{1}{2}$-coset and let Ax_2 be a $\frac{1}{3}$-coset. Consider now the coset Ax_1x_2. If $Ax_1x_2 = A$, then $x_1x_2 \in A$ and hence $x_1 = ax_2^{-1}$, for some $a \in A$. If follows that $C_A(x_1) = C_A(x_2^{-1}) = C_A(x_2)$, a contradiction, since $(A : C_A(x_1)) = 2$ and $(A : C_A(x_2)) = 3$. Now, since $x_1^2 \in A$ by lemma 3.3.12,

$$C_A(x_2) = C_A(x_1^2x_2) \supseteq C_A(x_1x_2) \cap C_A(x_1).$$

If $(A : C_A(x_1x_2)) = 2$, then $C_A(x_1x_2) \cap C_A(x_1)$ has index 2 or 4 in A and hence cannot be contained in $C_A(x_2)$ which has index 3 in A. It follows that Ax_1x_2 is a $\frac{1}{3}$-coset and clearly $Ax_1x_2 \neq Ax_2$. Let Ax_1x_2, Ax_2, and Ax_3 be the three distinct $\frac{1}{3}$-cosets of A in G. By the above argument the coset Ax_1x_3 is a $\frac{1}{3}$-coset and hence Ax_1x_3 must be equal to Ax_1x_2 or Ax_2, since clearly $Ax_1x_3 \neq Ax_3$.

Firstly, suppose that $Ax_1x_3 = Ax_2$. Therefore, $ax_1 = x_2x_3^{-1}$, for some $a \in A$. By lemma 3.3.12, $(ax_1)^2 = ax_1x_2x_3^{-1}$ belongs to A and thus $Ax_1x_2 = Ax_3$, a contradiction. Similarly, the assumption $Ax_1x_3 = Ax_1x_2$ leads to the contradiction that $Ax_2 = Ax_3$. Hence no $\frac{1}{2}$-coset can exist in this case and the lemma is proved.

(3.6.2) Lemma. The subgroup A is not normal in G.

Proof. Suppose, by way of contradiction that A is normal in G and consider first the possibility that G/A is cyclic of order 4. Let $G = \langle A, g \rangle$, where $g^4 \in A$, with $g = ax$, $a \in A$, and $x \in S_\alpha$, where α is a $\frac{1}{2}$-automorphism which inverts the elements of A. Now the subgroup $B = \langle C_A(x), ax \rangle$ is inverted by the $\frac{1}{2}$-automorphism $I_a\alpha$, and B has coset decomposition

$C_A(x) \cup C_A(x)(ax) \cup C_A(x)(ax)^2 \cup C_A(x)(ax)^3 \cup \ldots$ But $3|C_A(x)| = |A| > |B|$, which implies that $(ax)^3 = g^3 \in A$, a contradiction since $\langle Ag \rangle$ is cyclic of order 4.

Thus we may assume that $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4. If $C_A(x_1) = C_A(x_2)$, then $C_A(x_1) = C_A(x_1x_2) = Z$, the centre of G. In this case G/Z has 10 elements which satisfy $(Zg)^2 = Z$ and hence must be elementary Abelian. This is a contradiction since $|G/Z| = 12$.

There remains the possibility that $C_A(x_1)$, $C_A(x_2)$, and $C_A(x_1x_2)$ are distinct subgroups of index 3 in A. Let $A = \langle C_A(x_1), a_1 \rangle = \langle C_A(x_2), a_2 \rangle$, with $a_i^3 \in C_A(x_i)$, $[x_1, a_2] = 1 = [x_2, a_1]$, for $i = 1, 2$. Since A is assumed to be normal in G, $x_1^{-1}a_1x_1$ is c_1, a_1c_1, or $a_1^2c_1$, where c_1 lies in $C_A(x_1) = \langle Z, a_2 \rangle$ and Z is the centre of G. Now the possibility c_1 is easily excluded so assume that $x_1^{-1}a_1x_1 = a_1c_1$. Now $a_1 = x_1^{-2}a_1x_1^2 = a_1c_1^2$ and thus $c_1^2 = 1$. Finally, $x_1^{-1}a_1^2x_1 = (x_1^{-1}a_1x_1)^2 = a_1^2c_1^2 = a_1^2$, a contradiction.

Thus $x_i^{-1}a_ix_i = a_i^2c_i$, with $c_i \in C_A(x_i)$, $i = 1, 2$. An application of the Witt Identity gives

$$[x_1^{-1}, x_2^{-1}, a_2^{-1}]^{x_2} [x_2, a_2, x_1^{-1}]^{a_2^{-1}} [a_2^{-1}, x_1, x_2]^{x_1^{-1}} = 1$$

from which it follows that $[a_2, x_2] \in C_A(x_1)$. It follows that $c_2 \in C_A(x_1) \cap C_A(x_2) = Z$, and similarly $c_1 \in Z$.

Suppose now that $(x_1x_2)^{-1}a_1^{\ell}a_2^{m}(x_1x_2) = a_1^{\ell}a_2^{m}$. Using the relations just derived, a straightforward calculation gives $a_1^{\ell}a_2^{m} \in Z$, which implies that $C_A(x_1x_2) = Z$. This contradicts the fact that $(A : C_A(x_1x_2)) = 3$ and the lemma is established.

If $g^2 \in A$ for all g in G, then A is normal in G. Hence there exists $y \in G \setminus A$ such that $y^2 \notin A$. Now $y = ag$, for $a \in A$, $g \in S_\alpha$, where α is a $\frac{1}{2}$-automorphism inverting the elements of A. If we consider $B = \langle C_A(g), ag \rangle$, the usual argument gives $(ag)^3 = y^3 \in A$. Hence Ay and Ay^{-1} are distinct cosets. Without loss of generality, we may assume that $y \in S_\alpha$ since otherwise $I_a\alpha$ inverts y and the elements of B and the structure of G (mod B) is

similar to the structure of G (mod A).

Let Ax, with $x \in S_\alpha$, be the remaining $\frac{1}{3}$-coset of A in G. Since $(A)\alpha = A$, $(Ay)\alpha = Ay^{-1}$ we have $(Ax)\alpha = Ax = Ax^{-1}$. Thus $x^2 \in A$.

(3.6.3) Lemma. If Z is the centre of G then G/Z is isomorphic to the alternating group on four symbols.

Proof. Consider the coset Axy. Clearly Axy cannot be equal to any of the cosets A, Ay, and Ay^{-1}. Thus Axy = Ax and hence $C_A(x) = C_A(xy)$. Now, since $x^2 \in A$,

$$C_A(y) = C_A(x^2y) \supseteq C_A(x) \cap C_A(xy) = C_A(x).$$

It follows that $C_A(x) = C_A(y) = C_A(y^{-1}) = Z$, the centre of G. Thus G/Z has order 12. Now because $(G : A) = 4$, there is a homomorphism of G into S_4, the symmetric group on four symbols, whose kernel is Core A = Z. But A_4 is the only subgroup of order 12 in S_4 and hence G/Z is isomorphic to A_4.

Let $A = \langle Z, a \rangle$, with $a^3 \in Z$. Now $(x^{-1}ax)\alpha = (x^{-1}ax)^{-1}$, since $x^2 \in A$ and hence $x^{-1}ax \in S_\alpha$. We claim that A is self-normalizing since otherwise G/Z has a subgroup $N_G(A)/Z$ of index 2, contradicting the well known fact that A_4 has no subgroup of index 2. If follows that $x^{-1}ax \notin A$, since otherwise x normalizes A. Hence $x^{-1}ax = yz_2$ or $y^{-1}z_2$, with $z_2 \in Z$. Since y and y^{-1} can be interchanged, we define y by putting $x^{-1}ax = yz_2$.

Now, since Axy = Ax, $xy = a^*x$. By applying α and taking inverses we get $x^{-1}yx = az_1$ or a^2z_1, with $z_1 \in Z$. Since $y = x^{-2}yx^2$, the possibility $x^{-1}yx = a^2z_1$ is eliminated, and thus $x^{-1}yx = az_1$.

Finally, consider $y^{-1}ay$. Now $y^{-1}ay \notin S$, since $y^2 \notin A$, and clearly $y^{-1}ay$ is not contained in Ay. Thus $y^{-1}ay = axz_3$, a^2xz_3, $ay^{-1}z_3$, or $a^2y^{-1}z_3$. Straightforward calculations tell us that all these possibilities except the last lead to a contradiction. Thus $y^{-1}ay = a^2y^{-1}z_3$, with $z_3 \in Z$.

From the relation $[a, x^2] = 1$ it follows that $z_1z_2 = 1$ and thus $[a, x] = [x, y] = a^{-1}yz_2$. The relations $[a, y^3] = [a^3, y] = [a^3, x] = [x, y^3] = 1$ imply that $a^3 = y^3z_2^3$, $a^6 = y^6z_3^{-6}$, and thus $z_3^6 = z_2^{-6}$. We can now give a structure theorem.

(3.6.4) Theorem (Groups of type 19) Let G be a non-Abelian $\frac{1}{2}$-group such that three cosets of A in G are $\frac{1}{3}$-cosets, with A as in 3.3.1. Then $G = \langle A, x, y \rangle$, where A has index 4 in G. $C_A(x) = C_A(y) = Z$, and $A/Z = \langle Za \rangle$ has order 3, where Z is the centre of G. The group $G/Z = \langle Za, Zx, Zy \rangle$ is isomorphic to the alternating group on four symbols. G has commutator subgroup $\langle [a, x], [a, y] \rangle$, and the following relations hold:

$[a, x] = [x, y] = a^{-1}yz_2$, $[a, y] = ay^{-1}z_3$, $a^3 = y^3z_2^3$, $a^6 = y^6z_3^{-6}$,

where the elements x^2, y^3, z_2, and z_3 are all contained in Z.

Conversely, every such group has a $\frac{1}{2}$-automorphism α defined by

$$(za^ix^jy^k)\alpha = z^{-1}a^{-i}x^{-j}y^{-k},$$

for all $z \in Z$, $0 \leq i \leq 2$, $0 \leq j \leq 1$, $-2 \leq k \leq 2$.

(3.6.5) Example. The alternating group on four symbols is the simplest example of a group of type 19.

SECTION 3.7. The Case of Two $\frac{1}{4}$-cosets.

To complete our analysis of $\frac{1}{2}$-groups we must consider the case where two cosets of A in G are $\frac{1}{4}$-cosets and throughout this section let G denote such a non-Abelian $\frac{1}{2}$-group and α a $\frac{1}{2}$-automorphism which inverts the elements of A. We first consider the case where A is normal in G.

(3.7.1) Lemma. If A is normal in G then G/A is an elementary Abelian 2-group.

Proof. For all $x \in S_\alpha$, $a \in A$, $x^{-1}ax \in A$. An application of α gives $[x^2, a^{-1}] = 1$ and hence, by condition 3.3.11. III, $x^2 \in A$. Hence $(ax)^2 = ax^2(x^{-1}ax) \in A$ for all $a \in A$, $x \in S_\alpha$, and thus G/A is an elementary Abelian 2-group.

(3.7.2) Lemma. If A is normal in G then $(G : A) = 4$.

Proof. Let Ax_1 and Ax_2 be the distinct $\frac{1}{4}$-cosets of A in G. By lemma 3.7.1 Ax_1x_2 is a $\frac{1}{2}$-coset. Suppose now that there exists $x_3 \notin \langle A, x_1, x_2 \rangle$. Clearly $\langle A, x_1x_2, x_3 \rangle$ is a group of type 2 and $\langle A, x_1x_3, x_3 \rangle$ is a group of type

3. By the structure theorem 1.3.13 we have

$$[A, x_1x_2] = [A, x_3] = \langle z_3 \rangle, \quad \text{and} \tag{3.7.3}$$
$$[A, x_1x_3] = \langle z_{13} \rangle \neq \langle z_3 \rangle = [A, x_3].$$

But $\langle A, x_1x_2, x_1x_3, x_2x_3 \rangle$ is a group of type 2 and thus

$$[A, x_1x_3] = [A, x_1x_2],$$

which contradicts 3.7.3 and establishes the lemma.

We now examine in turn the various possibilities that can arise when A is normal in G. Assume firstly that $C_A(x_1) = C_A(x_2) = Z$, the centre of G. $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4 and Ax_1 and Ax_2 are the distinct $\frac{1}{4}$-cosets. Since A/Z is Abelian of order 4 it has two possible structures and each of these possibilities leads to a class of non-Abelian $\frac{1}{2}$-groups.

(3.7.4) Groups of type 20. For this type we assume that $A/Z = \langle aZ, a_{12}Z \rangle$ is elementary Abelian of order 4, with $[a, x_1x_2] = 1$. Now $[a, x_i^2] = 1 = [a^2, x_i]$ implies that $[a, x_i] \in C_A(x_i)$, $i = 1, 2$. Hence $[a, x_i] = z_i^*$ of order 2 in Z, $i = 1, 2$. But $[a, x_1x_2] = 1 = z_1^*z_2^*$, from which it follows that $z_1^* = z_2^* = z$.

Similarly, $[a_{12}, x_i^2] = 1 = [a_{12}^2, x_i]$ gives $[a_{12}, x_i] = z_i$, of order 2 in Z for $i = 1, 2$. Since $[a_{12}, x_1x_2] = z_1z_2 \neq 1$, we have $z_1 \neq z_2$. If $[x_1, x_2] \neq 1$ then $(a_{12}x_1x_2)\alpha = (a_{12}x_1x_2)^{-1}$, where α is a $\frac{1}{2}$-automorphism which inverts the elements of A and $x_1, x_2 \in S_\alpha$. An easy calculation gives $[x_1, x_2] = z_1z_2$ and hence $[a_{12}x_1, a_{12}x_2] = z_1^2z_2^2 = 1$. Thus in general we may choose the coset representatives of Ax_1 and Ax_2 to commute. Clearly $z \neq z_i$, since $[aa_{12}, x_i] \neq 1$, for $i = 1, 2$. However, z may be equal to z_1z_2. We can now give a structure theorem.

(3.7.5) Theorem. Let G be a non-Abelian $\frac{1}{2}$-group whose coset decomposition relative to A gives rise to two $\frac{1}{4}$-cosets Ax_1 and Ax_2. Suppose that A is normal in G, $C_A(x_1) = C_A(x_2) = Z$, the centre of G, and $A/Z = \langle Za, Za_{12} \rangle$ is elementary Abelian of order 4. Then $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4 and $G/Z = \langle Za, Za_{12}, Zx_1, Zx_2 \rangle$ is elementary Abelian

of order 16. G has commutator subgroup $G' = \langle z, z_1, z_2 \rangle$ which is elementary Abelian of order 4 or 8 and the following relations hold:

$[a, x_1] = z = [a, x_2]$; $[a_{12}, x_1] = z_1$; $[a_{12}, x_2] = z_2$; $[x_1, x_2] = 1$.

Conversely, every such group has a $\frac{1}{2}$-automorphism α defined by

$$(z^{*}a^{\varepsilon_1}a_{12}^{\varepsilon_2}x_1^{\delta_1}x_2^{\delta_2})\alpha = z^{*-1}a^{-\varepsilon_1}a_{12}^{-\varepsilon_2}x_1^{-\delta_1}x_2^{-\delta_2},$$

$\varepsilon_i, \delta_i = 0, 1$, $i = 1, 2$.

(3.7.6) Groups of type 21. For this type we assume that $C_A(x_1) = C_A(x_2) = Z$ and that $A/Z = \langle Za \rangle$ is cyclic of order 4. The relations $[a, x_i^2] = 1 \neq [a^2, x_i]$ imply that $[a, x_i] \notin Z$ and we can easily rule out the possibilities $[a, x_i] \in a^3Z$ and $[a, x_i] \in aZ$. Thus $[a, x_i] = a^2z_i$, with $z_i \in Z$, $i = 1,2$. Since $[a, x_i^2] = 1$, it follows that $[a, x_i]^4 = 1$, for $i = 1, 2$. Easy calculations show that $[a, x_1x_2] \neq 1$ implies that $[a, x_1] \neq [a, x_2]$, and $[a^2, x_1x_2] = 1$ implies that $[a, x_1]^2 = [a, x_2]^2$.

Now, since $(x_1x_2)^2 \in A$, an application of α gives $[(x_1x_2)^2, x_1] = 1$ and hence $(x_1x_2)^2 \in Z$. Thus, since x_1^2 and x_2^2 both belong to Z, $[x_1, x_2] \in Z$. If $a^ix_1x_2 \in S_\alpha$, where α is a $\frac{1}{2}$-automorphism which inverts the elements of A with $x_1, x_2 \in S_\alpha$, then $[x_2, x_1] = a^{3i}z_1^{2i}z_2^{i}$. Hence $i = 0$ and x_1 and x_2 commute.

(3.7.7) Theorem. Let G be a non-Abelian $\frac{1}{2}$-group whose coset decomposition relative to A gives rise to two $\frac{1}{4}$-cosets Ax_1 and Ax_2. Suppose that A is normal in G, $C_A(x_1) = C_A(x_2) = Z$, the centre of G, and $A/Z = \langle Za \rangle$ is cyclic of order 4. Then $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4. G has Abelian commutator subgroup $G' = \langle a^2z_1, a^2z_2 \rangle$ which is isomorphic to $C_4 \times C_2$. $G/Z = \langle Za, Zx_1, Zx_2 \rangle$ is a split extension of $D_4 (= \langle Za, Zx_1 \rangle)$ by an element Zx_2 of order 2 whose action is defined by the inversion of Za and Zx_1. The following commutator relations hold:

$[a, x_i] = a^2z_i$, $[a, x_i]^4 = 1$, $[a, x_1]^2 = [a, x_2]^2$, $[a, x_1x_2] = z_1z_2^{-1}$, $[x_1, x_2] = 1$, $z_i \in Z$, $i = 1, 2$.

Conversely, every such group has a $\frac{1}{2}$-automorphism α defined by

$$(za^i x_1^{\varepsilon_1} x_2^{\varepsilon_2})\alpha = z^{-1}a^{-i}x_1^{-\varepsilon_1}x_2^{-\varepsilon_2},$$

for all $z \in Z$, $0 \leq i \leq 3$, $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$.

We next turn our attention to the case where $C_A(x_1) \neq C_A(x_2)$, where Ax_1 and Ax_2 are the two $\frac{1}{4}$-cosets of A in G. If $C_A(x_2) \subset C_A(x_1x_2)$ then we have

$$C_A(x_1) = C_A(x_1x_2^2) \supseteq C_A(x_1x_2) \cap C_A(x_2) = C_A(x_2).$$

This contradiction shows that $C_A(x_2)$ is not contained in $C_A(x_1x_2)$, and thus $A = C_A(x_2)\, C_A(x_1x_2)$. Now Z, the centre of G, is equal to $C_A(x_1) \cap C_A(x_2) = C_A(x_2) \cap C_A(x_1x_2)$ and it follows that A/Z is Abelian of order 8. Now A/Z is non-cyclic since it has two distinct subgroups $C_A(x_1)/Z$ and $C_A(x_2)/Z$ of the same order. Thus we need only consider the cases $A/Z = C_2 \times C_2 \times C_2$ and $A/Z = C_4 \times C_2$.

(3.7.8) Groups of type 22. For this type we assume $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4, $A/Z = \langle Za, Zb, Zc \rangle$ is elementary Abelian of order 8. Put $C_A(x_1) = \langle Z, a \rangle$, $C_A(x_1x_2) = \langle Z, b, c \rangle$, and $C_A(x_2) = \langle Z, abc \rangle$. The relations $[a, x_2^2] = [a^2, x_2] = 1$ imply that $[a, x_2] \in C_A(x_2)$ and an application of the Witt identity gives $[a, x_2] \in C_A(x_1)$. Hence $[a, x_2] = z_3$ of order 2 in Z. By a similar argument $[b, x_i] = z_i$ of order 2 in Z ($i = 1, 2$). Since $[b, x_1x_2] = 1$ we have $z_1 = z_2 = z$. Similarly, $[c, x_i] = z_i^*$ of order 2 in Z and since $[c, x_1x_2] = 1$ we have $z_1^* = z_2^* = z^*$. In addition, $1 \neq [bc, x_1] = zz^*$, whence $z \neq z^*$. Finally, $[abc, x_2] = 1$ and hence $z_2zz^* = 1$.

Now if $[x_1, x_2] \neq 1$, $(ax_1x_2)\alpha = (ax_1x_2)^{-1}$, where α is the $\frac{1}{2}$-automorphism which inverts A and $x_1, x_2 \in S_\alpha$. Thus $[x_1, x_2] = z_3$ and hence $[ax_1, x_2] = z_3^2 = 1$. Hence we may choose the coset representatives of Ax_1 and Ax_2 to commute. Since $(x_1x_2)^2 \in A$, an application of α gives $(x_1x_2)^2 \in C_A(x_1) \cap C_A(x_2) = Z$, and since $[x_1, x_2] \in Z$, we have $x_1^2 \in Z$ and $x_2^2 \in Z$. We can now give the structure of G.

(3.7.9) Theorem. Let G be a non-Abelian $\frac{1}{2}$-group whose coset decomposition relative to A gives rise to two $\frac{1}{4}$-cosets Ax_1 and Ax_2. Suppose that A is

normal in G, $C_A(x_1) \neq C_A(x_2)$ and $C_A(x_1) \cap C_A(x_2) = Z$, the centre of G, with $A/Z = \langle Za, Zb, Zc \rangle$ elementary Abelian of order 8. Then $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4. G is nilpotent of class 2 with elementary Abelian commutator subgroup $G' = \langle z, z^* \rangle$ of order 4. $G/Z = \langle Za, Zb, Zc, Zx_1, Zx_2 \rangle$ is elementary Abelian of order 32 and the following relations hold:

$[a, x_1] = [abc, x_2] = [b, x_1x_2] = [c, x_1x_2] = 1$; $[b, x_1] = z$,
$[c, x_i] = z^*$, $i = 1, 2$ and $[a, x_2] = zz^*$; $[x_1, x_2] = 1$.

Conversely, every such group has a $\frac{1}{2}$-automorphism α defined by

$$(z_j a^{\varepsilon_1} b^{\varepsilon_2} c^{\varepsilon_3} x_1^{\delta_1} x_2^{\delta_2})\alpha = z_j^{-1} a^{-\varepsilon_1} b^{-\varepsilon_2} c^{-\varepsilon_3} x^{-\delta_1} x_2^{-\delta_2},$$

for all $z_j \in Z$, $\varepsilon_i, \delta_k = 0, 1$, $i = 1, 2, 3$, $k = 1, 2$.

(3.7.10) Groups of type 23. For this type we assume that $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4 and $A/Z = \langle Za, Zb \rangle$ is $C_2 \times C_4$, with $a^2 \in Z$ and $b^4 \in Z$. Let $C_A(x_1) = \langle a, Z \rangle$, $C_A(x_2) = \langle ab^2, Z \rangle$ and $C_A(x_1x_2) = \langle b, Z \rangle$. Now $[a^2, x_2] = 1 = [a, x_2^2]$ tells us that $[a, x_2] = z_2$ of order 2 in Z. Since $[ab^2, x_2] = 1$ we have $[b^2, x_2] = z_2$ and since $[b^2, x_1x_2] = 1$ we have $[b^2, x_1] = z_2$. Next, easy calculations give $[b, x_i] = b^2 z_i^*$, with $z_i^* \in Z$, $i = 1, 2$. Now the relation $1 = [b, x_1x_2]$ gives $(b^2 z_1^*)^2 z_2 z_1^{*-1} z_2^* = 1$, which, when combined with $[b^2, x_1] = z_2 = [b, x_1]^2$, gives $z_1^* = z_2^* = z$, and hence $[b, x_1] = [b, x_2]$ of order 4.

Finally, if $[x_1, x_2] \neq 1$ we have $(ax_1x_2)\alpha = (ax_1x_2)^{-1}$ and thus $[x_1, x_2] = z_2$. But then $[ax_1, x_2] = z_2^2 = 1$, showing that we may choose the coset representatives of Ax_1 and Ax_2 to commute. Again we give a structure theorem.

(3.7.11) Theorem. Let G be a non-Abelian $\frac{1}{2}$-group whose coset decomposition relative to A gives rise to two $\frac{1}{4}$-cosets Ax_1 and Ax_2. Suppose that A is normal in G, $C_A(x_1) \neq C_A(x_2)$, and $C_A(x_1) \cap C_A(x_2) = Z$, the centre of G, with $A/Z = \langle Za, Zb \rangle$ isomorphic to $C_2 \times C_4$. The $G/A = \langle Ax_1, Ax_2 \rangle$ is elementary Abelian of order 4. G has Abelian commutator subgroup $G' = \langle b^2 z \rangle$ which is cyclic of order 4. $G/Z = \langle Za, Zb, Zx_1, Zx_2 \rangle$ has order 32 subject to

the relations:

$[a, x_1] = [ab^2, x_2] = [b, x_1x_2] = [x_1, x_2] = 1;$

$[a, x_2] = [b^2, x_2] = [b^2, x_1] = z_2$;

$[b, x_1] = [b, x_2] = b^2z$, and $b^4z^2 = z_2$. The elements a^2, b^4, x_1^2, x_2^2, z, z_2, and $(x_1x_2)^2$ all lie in Z.

Conversely, any such group has a $\frac{1}{2}$-automorphism α defined by

$$(z^*a^ib^jx_1^{\epsilon_1}x_2^{\epsilon_2})\alpha = z^{*-1}a^{-i}b^{-j}x_1^{-\epsilon_1}x_2^{-\epsilon_2},$$

for all z^* in Z, $0 \leq i, \epsilon_1, \epsilon_2 \leq 1$, $0 \leq j \leq 3$.

All that now remains is to consider the case where A is not normal in G.

(3.7.12) Lemma. If A is not normal in G then $(G : A) = 4$.

Proof. We first rule out the possibility that $(G : A) = 3$. Suppose $G = A \cup Ax \cup Ax^2$. If α is a $\frac{1}{2}$-automorphism which inverts the elements of A, we may suppose that x belongs to S_α, since otherwise $ax \in S_\alpha$ for some $a \in A$, and then the $\frac{1}{2}$-automorphism $I_a\alpha$ inverts A, ax, and $(ax)^2$. Since Ax and Ax^2 are $\frac{1}{4}$-cosets by hypothesis, $C_A(x) = C_A(x^2) = Z$, the centre of G. Let $A = Z \cup Za_1 \cup Za_2 \cup Za_1a_2$, where we do not exclude the possibility that $a_2 = a_1^2$.

Now $x^{-1}a_1x$ does not belong to S_α since this would imply that $[x^2, a_1] = 1$. Hence $x^{-1}a_1x = a_1^*x^2$ and similarly $x^{-1}a_2x = a_2^*x^2$ and $x^{-1}a_1a_2x = a_{12}^*x^2$, for a_1^*, a_2^*, $a_{12}^* \in A$. But then $a_1^*x^2a_2^*x^2 = a_{12}^*x^2$, which implies that $x^2 \in A$, a contradiction.

Next we show that $(G : A) > 4$ is not possible. Suppose therefore that $(G : A) = n > 4$ and let Ax_1 and Ax_2 be the distinct $\frac{1}{4}$-cosets. By lemma 3.3.12, the elements of every other coset of A in G normalize A and hence $n = (G : A) = (G : N_G(A))(N_G(A) : A) \geq (G : N_G(A))(n - 2)$. This is a contradiction for $n > 4$ since $(G : N_G(A))$ is an integer greater than 1.

Hence $(G : A) = 4$ and thus there is a homomorphism of G into a subgroup of S_4 whose kernel K is Core A (the largest normal subgroup of G contained in A). Now we have $Z \trianglelefteq K \subset A \subset G$. If $K = Z$ we obtain a

contradiction because then G/Z has order at least 16 and hence $|G/K|$ cannot divide $|S_4| = 24$. It now follows that G/K has order 8 and hence is isomorphic to a Sylow subgroup of S_4 which is D_4.

Let $G/K = \langle xK, aK \rangle$, where $x^4, a^2 \in K$ and $a^{-1}xa = x^{-1} \pmod{K}$ and $a \in A \setminus K$. It is clear that $C_A(x) = C_A(x^3) = Z$ and $K = C_A(x^2)$. Consider $\langle K, x^2 \rangle = B$ which is elementwise inverted by α. We have $|A| = |B|$ and the cosets Ba and Bx are $\frac{1}{2}$-cosets. Thus the remaining coset of B in G is an empty-coset and hence G has already been classified in Section 3.4. This completes our analysis of $\frac{1}{2}$-groups.

CHAPTER 4. MEASURES OF COMMUTATIVITY

SECTION (4.1) Introduction

We have already defined $\ell(G)$ for a finite group G and in previous chapters examined those groups for which $\ell(G)$ is large. It was no surprise to find that such groups are "nearly Abelian" i.e. they have large Abelian subgroups and small commutator subgroups. Since $\ell(G) = 1$ if and only if G is Abelian, we use the size of $\ell(G)$ as a measure of the commutativity of G.

In a doctoral thesis at the University of California in 1969, K. S. Joseph [5] used the function $R(G) = k(G)/|G|$, where $k(G)$ is the number of conjugacy classes in G, as a measure of the commutativity of G. It is clear that $R(G) = 1$ if and only if G is Abelian and it is easy to show that $R(G)$ is the probability that a pair of elements chosen at random in G will commute with each other. In this chapter we show that if $\ell(G)$ is large then $R(G)$ is also large. For the groups of type 1 to 23 we either calculate $R(G)$ or give a bound for its value.

The connection between $\ell(G)$ and $R(G)$ is based on the following intuitive notion. The number $\ell(G)$ is the maximum proportion of elements of G which are mapped onto their inverses by an automorphism. If β is the mapping defined by $(x)\beta = x^{-1}$ for all x in G, then $R(G)$ is the proportion of pairs of elements (x_i, x_j) which satisfy the automorphism property $(x_i x_j)\beta = (x_i)\beta(x_j)\beta$.

SECTION 4.2. Notation and Results

We use the following notation and results from Joseph's thesis and other sources.

(4.2.1) Definition. Let $\{n_i | i = 1, \ldots, v\}$ be the orders of the conjugacy classes of G. The conjugate type of $G = c.t.(G) = (n_0 = 1, n_1, \ldots, n_v)$, where the n_i are distinct.

(4.2.2) Definition. Let $\{m_j | j = 1, \ldots, \mu\}$ be the degrees of the

absolutely irreducible representations of G. The degree type of G = d.t.(G) = $(m_0 = 1, m_1, \ldots, m_\mu)$, where the m_j are distinct.

(4.2.3) Known Results

(i) $n_i | (G : Z)$ and $n_i < (G : Z)$, where Z is the centre of G. Also, $n_i \leq |G'|$.

(ii) If A is an Abelian normal subgroup of G, Ito [4] has shown that $m_j | (G : A)$ and Isaacs and Passman [2] have shown that $m_j^2 \leq (G : Z)$.

(iii) If c.t.(G) = (1, n) then $R(G) = \frac{1}{n}(1 + \frac{n-1}{(G:Z)})$.

(iv) $R(G) \geq \frac{1}{|G'|}(1 + \frac{|G'|-1}{(G:Z)})$, with equality if and only if c.t.(G) = (1, $|G'|$).

(v) $R(G) > \frac{1}{(G:Z)}(1 + \frac{(G:Z)-1}{(G:Z)})$.

(vi) Let p denote the smallest prime divisor of $|G|$. Then $R(G) \leq \frac{1}{p}(1 + \frac{p-1}{(G:Z)})$, with equality if and only if c.t.(G) = (1, p).

(vii) Suppose d.t.(G) = (1, m). Then

$$R(G) = \frac{1}{m^2}(1 + \frac{m^2-1}{|G'|}).$$

(viii) Let p denote the smallest prime divisor of G . Then $R(G) \leq \frac{1}{p^2}(1 + \frac{p^2-1}{|G'|})$, with equality if and only if d.t.(G) = (1, p).

(4.2.4) Definition. G_1 is said to be isoclinic to G_2 if

(i) $G_1/Z(G_1)$ is isomorphic to $G_2/Z(G_2)$,

(ii) G_1' is isomorphic to G_2', and

(iii) The isomorphisms ψ and ϕ in (i) and (ii) respectively can be chosen so that $[x_1, y_1]\phi = [x_2, y_2]$, for all $x_1, y_1 \in G_1$ whenever $(x_1 Z(G_1))\psi = x_2 Z(G_2)$ and $(y_1 Z(G_1))\psi = y_2 Z(G_2)$.

Joseph [5] has shown that if G_1 and G_2 are isoclinic, then $R(G_1) = R(G_2)$.

(4.2.5) Result. Isaacs and Passman [3] have shown that if G is

finite and either (i) G has a normal Abelian subgroup of index p or (ii) G/Z has order p^3 and exponent p, then d.t.(G) = (1, p).

We arenow in a position to calculate R(G), where G is a group of type 1 to type 23.

SECTION 4.3. Values of R(G).

(4.3.1) $>\frac{1}{2}$-groups. If G has type 1, then G = A $\cup$ Ax, where A is Abelian and q = (A : $C_A(x)$) = (A : Z). Elementary calculations give R(G) = $\frac{q+3}{4q}$ and hence R(G) > $\frac{1}{4}$. Recall that $\ell(G) = \frac{q+1}{2q}$.

If G has type 2, then the conjugacy type of G is (1, 2) since |G'| = 2. Formula 4.2.3. (iv) now gives $R(G) = \frac{1}{2} + \frac{1}{2^{2k+1}}$, where k can be any positive integer. Recall $\ell(G) = \frac{2^{k+1}}{2^{k+1}}$.

If G has type 3 we use the fact that any two groups of type 3 are isoclinic and thus $R(G) = R(D_4 \times D_4) = (R(D_4))^2 = \frac{25}{64}$, since $D_4 \times D_4$ has type 3. We recall that $\ell(G) = \frac{9}{16}$.

(4.3.2) $\frac{1}{p}$-groups. If G has type 4, then |G'| = p, c.t.(G) = (1, p) and G/Z has order p^{2k}. Formula 4.2.3 (iv) now gives $R(G) = \frac{1}{p} + \frac{p-1}{p^{2k+1}}$.

If G has type 5, by 4.2.5, d.t.(G) = (1, p). Hence, by 4.2.3 (viii), $R(G) = \frac{1}{p^2}\left(1 + \frac{p^2-1}{|G'|}\right)$. Now $|G'| = p^2$ or p^3 and hence $R(G) = \frac{1}{p^4}(2p^2 - 1)$ or $\frac{1}{p^5}(p^3 + p^2 - 1)$.

If G has type 6, then by 4.2.5, d.t.(G) = (1, p). Thus $R(G) = \frac{1}{p^2}\left(1 + \frac{p^2-1}{|G'|}\right)$ and hence $R(G) > \frac{1}{p^2}$.

(4.3.3) $\frac{1}{2}$-groups. Finally, we calculate or give bounds for the value of R(G) when $\ell(G) = \frac{1}{2}$.

If G has type 7, R(G) = 1 and if G has type 8 then G is also of type 1.

If G has type 9, formula 4.2.3(iv) tells us that $R(G) > \frac{23}{128}$. If G has type 10 or type 11, similarly we have $R(G) > \frac{23}{128}$.

If G has type 12, formula 4.2.3 (iv) implies that $R(G) \geq \frac{19}{64}$. Again, if G has type 13 or type 14, $R(G) \geq \frac{19}{64}$.

If G has type 15, $(G: Z) = 8 \geq m_j^2$. Hence d.t.(G) = (1, 2) and $R(G) = \frac{1}{4}(1 + \frac{3}{|G'|})$. Hence $R(G) = \frac{7}{16}$ or $\frac{11}{32}$ in this case.

Groups of type 16 coincide with groups of type 2.

If G has type 17, it is clear that $R(G) = \frac{7}{16}$.

If G has type 18 then G is isoclinic to $D_4 \times D_3$. Hence $R(G) = R(D_4) \times R(D_3) = \frac{5}{16}$.

If G has type 19, formula 4.2.3 (v) tells us that $R(G) > \frac{23}{144}$.

If G has type 20 or type 21, then $R(G) > \frac{23}{128}$.

Finally, if G has type 22 or type 23, $R(G) \geq \frac{19}{64}$.

SECTION 4.4. R(G) and $\ell(G)$.

In this section we mention some connections between R(G) and $\ell(G)$ using the results of Joseph. It is clear that $R(G) = 1 = \ell(G)$ if and only if G is Abelian. Next, $R(G) = \frac{5}{8}$ if and only if $(G : Z(G)) = 4$ if and only if $\ell(G) = \frac{3}{4}$, and these are the maximum possible values of R(G) and $\ell(G)$ for non-Abelian groups. It is easy to show that $\ell(G) = \frac{2}{3}$ if and only if $R(G) = \frac{1}{2}$ and in this case $|G'| = 3$ and $(G : Z(G)) = 6$.

It seems significant that R(G) and $\ell(G)$ are both "quantised" i.e. if $1 > R(G) > \frac{1}{2}$ then $|G'| = 2$ and $R(G) = \frac{1}{2} + \frac{1}{2^{2k+1}}$, and if $\ell(G) > \frac{1}{2}$ then $\ell(G) = \frac{q+1}{2q}$, where k and q are positive integers. Joseph (personal communication) has shown that there are no groups G with $\frac{7}{16} < R(G) < \frac{1}{2}$, showing the significance of groups of type 17. If $G \in G_p$, then $R(G) = \frac{1}{p}$ is not possible unless p = 2.

The function R(G) has the following properties:

(i) R is multiplicative i.e. $R(G_1 \times G_2) = R(G_1)R(G_2)$.

(ii) If H is a subgroup of G then $R(H) \geq R(G)$, and if H is normal in G, $R(G/H) \geq R(G)$. Hence subgroups and factor groups are at least as Abelian as the group itself.

(iii) If G_1 is isoclinic to G_2, then $R(G_1) = R(G_2)$.

We conjecture that analogues of these results hold for the function $\ell(G)$, but suspect that the proofs may be quite difficult. If $\mathrm{Aut}\,(G_1 \times G_2) = \mathrm{Aut}\,(G_1) \times \mathrm{Aut}\,(G_2)$, then clearly $\ell(G_1 \times G_2) = \ell(G_1)\ell(G_2)$, but we have been unable to prove the general result even when one of the groups is Abelian. However, $\ell(A \times B) = \ell(A)\ell(B)$ when A is Abelian and B is a $>\frac{1}{2}$-group. If H is a characteristic subgroup of G, then the method of proof of 1.2.2 enables us to prove that $\ell(H) \geq \ell(G)$ and $\ell(G/H) \geq \ell(G)$.

Examination of the structure theorems for $>\frac{1}{2}$-groups, $\frac{1}{p}$-groups, and $\frac{1}{2}$-groups gives much evidence for the conjecture that if G_1 and G_2 are isoclinic then $\ell(G_1) = \ell(G_2)$.

Finally, we note the following anomaly. Let S_3 be the symmetric group on 3 symbols and let G be the product of two dihedral groups of order 8 with centres amalgamated. Then $R(G) = \frac{17}{32} > \frac{1}{2} = R(S_3)$. However, $\ell(G) = \frac{5}{8} < \frac{2}{3} = \ell(S_3)$.

CHAPTER 5. C-SETS

SECTION (5.1) Introduction.

In Chapter 4 we have shown how $\ell(G)$ serves as a measure of commutativity of a finite group G. However, $\ell(G)$ is not always a good measure of commutativity as the following lemma and example show.

(5.1.1) Lemma. If both $|\text{Aut } G|$ and $|G|$ are odd then $\ell(G) = 1/|G|$.

Proof. Let α be any automorphism of G and suppose that $g \in S_\alpha$. Since $|\text{Aut } G|$ is odd, α has order $2n+1$, for some integer n. Now

$$g = (g)\alpha^{2n+1} = ((g)\alpha^{2n})\alpha = g(\alpha) = g^{-1}.$$

Thus, since $|G|$ is odd, $g = 1$. Hence $|S_\alpha| = 1$ for all $\alpha \in \text{Aut } G$ and it follows that $\ell(G) = 1/|G|$.

(5.1.2) Example. The following example, due to G. A. Miller [12] shows that there exists a group of odd order whose automorphism group also has odd order. Let $G = \langle a, b, c \rangle$ where a, b, and c have orders p^4, p^3, and p^2 respectively and p is an odd prime. In addition, $[c, a] = a^{p^3}$, $[c, b] = c^p$, and $[b, a] = b^{p^2}$. Then G has order p^9 and Aut G is also a p-group. Thus by lemma 5.1.1, $\ell(G) = 1/|G|$.

In cases like this $\ell(G)$ gives us no information at all about the commutativity of G. The difficulty lies in the peculiarity of the automorphism group of G, so in the next section we define a new measure of commutativity which does not depend on automorphisms. Recall that if $S_\alpha = \{x \in G | (x)\alpha = x^{-1}, \alpha \in \text{Aut } G\}$, then given $x_1, x_2 \in S_\alpha$, $x_1x_2 \in S_\alpha$ if and only if $x_1x_2 = x_2x_1$.

SECTION (5.2) Properties of C-Sets.

(5.2.1) Definition. A C-set S of a finite group G is a subset S of G which has the following property:

given $s_1, s_2 \in S$, $s_1s_2 \in S$ if and only if $s_1s_2 = s_2s_1$.

(5.2.2.) Definition If S^* is a C-set of maximum order in G then $b(G) = |S^*|/|G|$.

Obviously $b(G) = 1$ if and only if G is Abelian, so we use $b(G)$ as another measure of the commutativity of G. We note that if $|G| > 1$ then $b(G) > 1/|G|$, since an Abelian subgroup is always a non-trivial C-set. It is clear that if $s \in S$ then $\langle s \rangle \subset S$, where S is a C-set of G.

(5.2.3) Lemma. If S^* is a C-set of maximum order in G, then $S^* \supset Z(G)$, the centre of G.

Proof. Consider $S^*Z(G)$. If $S^* \supsetneq Z(G)$ then $S^*Z(G)$ is clearly a C-set which contains S^* properly. This contradicts the definition of S^* and establishes the lemma.

For the remainder of this section we let G denote a non-Abelian group in G_p, where p is a prime.

(5.2.4) Theorem. If G is a non-Abelian group in G_p, then $b(G) \leq \frac{2p-1}{p^2}$, with equality if and only if $(G : Z(G)) = p^2$.

Proof. Let S^* be a C-set of maximum order in G and let A be a subgroup of maximum order in S^*. For $x \notin A$, if $Ax \cap S^*$ is not empty, choose $x \in S^*$. Now for $a \in A$, $ax \in S^*$ if and only if $ax = xa$ and thus $Ax \cap S^* = (C_A(x))x$. If $C_A(x) = A$, then $\langle A, x \rangle$ is a subgroup contained in S^* having order greater than that of A. Hence $|S^* \cap Ax| = |C_A(x)| \leq \frac{1}{p}|A|$. It follows that

$$|S^*| \leq |A| + \{(G : A) - 1\} \frac{1}{p}|A| = \frac{1}{p}|G| + |A| \left(1 - \frac{1}{p}\right).$$

Since $(G : A) \geq p$, it follows that

$$|S^*| \leq \frac{1}{p}|G| + \frac{1}{p}|G| \left(1 - \frac{1}{p}\right) = |G| \frac{2p-1}{p^2}.$$

Thus $b(G) \leq \frac{2p-1}{p^2}$.

If $b(G) = \frac{2p-1}{p^2}$, the above analysis shows that $(G : A) = p$ and $(A : C_A(x)) = p$ for all $x \notin A$. Let $G = \langle A, x \rangle$ with $x^p \in A$. It is clear that $C_A(x) = C_A(x^2) = \ldots = C_A(x^{p-1}) = Z(G)$.

Hence $(G : Z(G)) = p^2$.

Conversely, if $G/Z = \langle Za, Zx \rangle$ is non-cyclic of order p^2 then $\langle z, a \rangle = A$, an Abelian subgroup of index p in G. Then the set $A \cup \bigcup_{i=1}^{p} (C_A(x^i))x^i$ is a C-set of order $(\frac{2p-1}{p^2})|G|$, and thus $b(G) = \frac{2p-1}{p^2}$.

This theorem makes an interesting comparison with the following theorem of Joseph [5] :

If G is a non-Abelian group in G_p then $R(G) \leq \frac{p^2 + p - 1}{p^3}$, with equality if and only if $(G : Z(G)) = p^2$.

SECTION 5.3. Groups with $b(G) > \frac{1}{2}$.

We complete this chapter by deriving some results on groups with $b(G) > \frac{1}{2}$. (The following proof is based on an idea of Dr. T. J. Laffey.)

(5.3.1) Theorem. If $b(G) > \frac{1}{2}$ then G is a soluble group.

Proof. Let S be a C-set in G for which $|S| > \frac{1}{2}|G|$. If the elements of S are involutions then G is soluble by the results of Chapter 1. Assume therefore that there exists $y \in S$ such that $y^2 \neq 1$.

Now $|G| \geq |S \cup yS \cup y^2S| =$

$$|S| + |yS| + |y^2S| - |S \cap yS| - |S \cap y^2S| - |yS \cap y^2S| + |S \cap yS \cap y^2S|.$$

Now consider $w \in S \cap yS$. It is clear that $w = ys = sy$, with $s \in S$. It follows that $wy = ysy = yw$, and hence $w \in C_G(y)$. Thus $S \cap yS \subseteq C_G(y)$ and similarly $S \cap y^2S \subseteq C_G(y^2)$. Obviously $|yS \cap y^2S| = |S \cap yS|$. Next, let $w \in S \cap yS$ with $wy = yw$. It follows that $y^{-2}w = wy^{-2}$, with $y^{-2} \in S$. Hence $y^{-2}w \in S$ and thus $w \in y^2S$. Finally,

$$S \cap yS = S \cap yS \cap y^2S.$$

Equation 5.3.2 now gives $|G| \geq 3|S| - |S \cap yS| - |S \cap y^2S|$.

Using the relations $|S| > \frac{1}{2}|G|$, $C_G(y) \subseteq C_G(y^2)$ and $S \cap yS \subseteq C_G(y)$, we find

$|C_G(y^2)| > \frac{1}{4}|G|$, for all $y \in S$ and hence $|C_G(y^2)| \geq \frac{1}{3}|G|$.

Recall that if $(G : M) = m$ and Core $M = \bigcap_{x \in G} x^{-1}Mx$, then G/Core M is isomorphic to a subgroup of S_m, the symmetric group on m symbols. Thus in this case G/Core $C_G(y^2)$ is isomorphic to a subgroup of S_3. Since the

second derived group of S_3 is the identity, it follows that $G'' \subseteq \text{Core } C_G(y^2)$ for all $y \in S$, where G'' is the second derived group of G. Hence if $W = \bigcap_{y \in S} \text{Core } C_G(y^2)$, then $G'' \subseteq W$.

Finally, consider $C_G(W)$. Let $X = \{x\, C_G(W) | x \in S\}$. X, considered as a subset of G contains at least half the elements of G since $S \subset X$. Hence X, considered as a subset of $G/C_G(W)$, contains at least half the elements of $G/C_G(W)$. But if $x \in S$ then $x^2 \in C_G(W)$ and thus X consists of involutions in $G/C_G(W)$. Hence as least half the elements of $G/C_G(W)$ are involutions and by the results of Chapter 1, section 1.4, $G'' \subseteq C_G(W)$. Thus $G'' \subseteq W \cap C_G(W) = Z(W)$ the centre of W. It follows that $G''' = 1$ and so G is soluble of derived length at most three.

We proceed to give some results and the partial structure of groups with $b(G) > \frac{1}{2}$. Since $\ell(G) > \frac{1}{2}$ implies $b(G) > \frac{1}{2}$ we would expect that many of the methods of Chapter 1 apply, and this is indeed the case.

Let G be a group for which $b(G) > \frac{1}{2}$ and let S be a C-set of maximum order in G for which $|S| > \frac{1}{2}|G|$. Let A be a subgroup of maximum order in S. A is clearly Abelian and if $s \in S \setminus A$, then $As \cap S = C_A(s)s$. Obviously $|C_A(s)| = |As \cap S| \leq \frac{1}{2}|A|$. Hence every coset of A in G contains elements of S and we write

(5.3.3) $\quad G = A \cup As_2 \cup \ldots \cup As_n,\ s_i \in S,\ 1 \leq i \leq n,\ s_1 = 1,$

(5.3.4) $\quad$ and $|S| = |A| + \sum_{i=2}^{n} |C_A(s_i)|.$

Let $q_i = (A : C_A(s_i))$, $1 \leq i \leq n$. The condition $|S| > \frac{1}{2}|G|$ tells us that

(5.3.5) $$\sum_{i=2}^{n} \left(\frac{1}{2} - \frac{1}{q_i}\right) < \frac{1}{2}.$$

The inequality (5.3.5) tells us that relative to a suitable ordering of the cosets of A in G one of the following conditions must apply, where $(G : A) = n$.

I $n = 2$;

II $n \geq 3$, $q_1 = 2$, $i = 2, \ldots, n$;

(5.3.6) III $n \geq 3$, $q_2 \geq 3$, $q_i = 2$, $i = 3, \ldots, n$;

IV $n \geq 3$, $q_2 = 3$, $q_3 = 4$ or 5, $q_i = 2$, $i = 4, \ldots, n$;

V $n \geq 3$, $q_2 = q_3 = 3$, $q_i = 2$, $i = 4, \ldots, n$;

Firstly, if $n = 2$ then $G = A \cup As$ and $S = A \cup (C_A(s))s$. Thus $b(G) = \frac{q+1}{2q}$, where $(A : C_A(s)) = q$. Clearly any non-Abelian group G with an Abelian subgroup of index 2 has such a C-set and $b(G) = \frac{q+1}{2q} > \frac{1}{2}$.

(5.3.7) Lemma. If $(A : C_A(s)) = 2$, then $s^2 \in A$, where $s \in S$.

Proof. If $s^2 \notin A$, then $\langle C_A(s), s \rangle$ is contained in S and has order greater than that of A, a contradiction.

Similarly, if in Case III $(A : C_A(s_2)) = q_2 \geq 3$, we have $s_2^2 \in A$ and hence $s^2 \in A$, for all $s \in S$.

In like manner in case IV, $s^2 \in A$, for all $s \in S$.

(5.3.8) Lemma. There are no groups G which satisfy condition 5.3.6.IV.

Proof. Let $G = A \cup As_2 \cup As_3 \ldots$, where $(A : C_A(s_2)) = 3$ and $(A : C_A(s_3)) = 4$ or 5. Consider the coset As_2s_3. It is clear that $As_2s_3 = As_2$ or $(A : C_A(s_2s_3)) = 2$. Now,

$C_A(s_3) = C_A(s_2^2 s_3) \supseteq C_A(s_2) \cap C_A(s_2s_3)$, a contradiction, since $(A : C_A(s_3)) = 4$ or 5 and $(A : C_A(s_2) \cap C_A(s_2s_3)) = 3$, 6, or 9.

In contrast with groups for which $\ell(G) > \frac{1}{2}$, there exist groups which satisfy condition 5.3.6 V and $b(G) > \frac{1}{2}$.

(5.3.9) Theorem. Let G be a group which satisfies condition 5.3.6 V and $b(G) > \frac{1}{2}$. Then

(i) $(G : A) = n = 3$

(ii) $G/Z(G)$ has order 9, and

(iii) $b(G) = \frac{5}{9}$.

Conversely, every such group G satisfying (i) and (ii) has $b(G) = \frac{5}{9}$.

Proof. Suppose that As_1 and As_2 are distinct cosets with $(A : C_A(s_1) = (A : C_A(s_2)) = 3$ and let As be a coset such that $(A : C_A(s)) = 2$, with $s_1, s_2, s \in S$, and S a C-set for which $|S| > \frac{1}{2}|G|$. By lemma 5.3.7 $s^2 \in A$ and hence

(5.3.10) $C_A(s_1) = C_A(s^2 s_1) \geq C_A(s) \cap C_A(ss_1)$.

Clearly $Ass_1 \neq A$, and if $(A : C_A(ss_1)) = 2$ we contradict 5.3.10. Thus $(A : C_A(ss_1)) = 3$ and thus $Ass_1 = As_2$. Similarly,

$$C_A(ss_1^2) \geq C_A(ss_1) \cap C_A(s_1),$$

and thus $(A : C_A(ss_1^2)) = 3$. Hence $Ass_1^2 = As_1$ or Ass_1 and each of these possibilities easily leads to a contradiction. It follows that $(G : A) = 3$.

Now if $G = A \cup Ax \cup Ax^2$, $C_A(x) = C_A(x^2) = Z(G)$ and $G/Z(G)$ has order 9, where Z is the centre of G. The rest of the proof is now obvious and corresponds to theorem 5.2.4 with $p = 3$.

It is interesting to note that the groups of theorem 5.3.9 may have odd order e.g. the non-Abelian group of order 27 and exponent 3, in contrast with the situation when $\ell(G) > \frac{1}{2}$.

Finally we derive a numerical restriction on the value of $b(G)$ when $b(G) > \frac{1}{2}$.

(5.3.11) Theorem. If $b(G) > \frac{1}{2}$, then $b(G) = \frac{q+1}{2q}$ for some positive integer q.

Proof. Our method of proof is to examine the various possibilities arising from 5.3.6. Possibility I has already been covered, lemma 5.3.8 has eliminated possibility IV, and for possibility V, $b(G) = \frac{5}{9}$. If possibility II arises, $b(G) = \frac{n+1}{2n}$, where $(G : A) = n$. In case III, $q_2 = (A : C_A(s_1)) \geq 3$, $q_i = 2$, $3 \leq i \leq n$. We claim that q_2 is even. For if q_2 is odd and As, $s \in S$, is a coset for which $(A : C_A(s)) = 2$ then $C_A(s_1) = C_A(s_1 s^2) \geq C_A(s_1 s) \cap C_A(s)$. Examination of the possibilities shows that $(A : C_A(s_1 s) \cap C_A(s))$ is even, a contradiction. Thus

$|S| = |A| + (n - 2)|A|\frac{1}{2} + \frac{1}{q_2}|A|$. Thus $|S|/|G| = \frac{nq_2 + 2}{2nq_2} = \frac{q + 1}{2q}$ where $q = \frac{nq_2}{2}$. Thus b(G) is always of the form $\frac{q + 1}{2q}$ and the proof is completed.

REFERENCES

1. Gorenstein, D., Finite Groups (Harper & Row 1968).

2. Isaacs, I. M. and Passman, D. S., "A characterization of groups in terms of the degrees of their characters." Pacific Journal of Mathematics, 15, 877-903 (1965).

3. ————————, "Groups whose irreducible representations have degrees dividing p^e." Illinois Journal of Mathematics 8, 446-457 (1964).

4. Ito, N., "On finite groups with given conjugate types I", Nagoya MathematicalJournal 6, 17-28 (1953).

5. Joseph, K. S., "Commutativity in Non-Abelian Groups", Doctoral Thesis, University of California, Los Angeles (1969).

6. Kovács L. G. and Wall G. E., "Involutory automorphisms of groups of odd order and their fixed point groups", Nagoya Math. Journal 27, 113-120 (1966).

7. Manning, W. A., "Groups in which a large number of operators may correspond to their inverses." Trans. Amer. Math. Soc. 7, 233-240 (1906).

8. Miller, G. A., "Non-Abelian groups admitting more than half inverse correspondences." Proc. Nat. Acad. Sci. 16, 168-172 (1930).

9. ————————, "Groups of order 2^m which contain a relatively large number of operators of order two", Amer. Journ. Math. 42, 1-10 (1920).

10. ————————, "Isomorphisms of a group whose order is a power of a prime", Trans. Amer. Math. Soc. 12, 387-402 (1911).

11. ————————, "Non-Abelian Groups of odd prime power order which admit a maximal number of inverse correspondences in an automorphism", Proc. Nat. Acad. Sci. 15, 859-862 (1929).

12. ————————, "A group of order p^m whose group of isomorphisms is of order p^{α}", Messenger of Mathematics 43, 126-128 (1913).

13. Wall, C. T. C.,"On Groups consisting mostly of involutions", Proc. Cambridge Philos. Soc., 67, 251-262 (1970).

14. Ward, J. N., "Involutory automorphisms of groups of odd order", Jour. Australian Math. Soc. 6, 480-494 (1966).

15. Zassenhaus, H., The Theory of Groups (Chelsea 1956).

16. Liebeck, H. and MacHale, D., "Groups with automorphisms inverting most elements", Math. Z. 124, 51 - 63 (1972).

17. ———————————— "Groups of odd order with automorphisms inverting many elements". To appear J. London Math. Soc.